VŠB – Technická univerzita Ostrava
Fakulta metalurgie a materiálového inženýrství
Katedra materiálů a technologií pro automobily

# Zabezpečení elektromobilu

# Security of electric vehicle

Student: Dominik Tajchman
Vedoucí bakalářské práce: Ing. Martin Juránek, Ph.D.

Ostrava 2015

VŠB - Technická univerzita Ostrava
Fakulta metalurgie a materiálového inženýrství
Katedra materiálů a technologií pro automobily

# Zadání bakalářské práce

Student: **Dominik Tajchman**

Studijní program: B3923 Materiálové inženýrství

Studijní obor: 3911R034 Materiály a technologie pro automobilový průmysl

Téma: Zabezpečení elektromobilu
Security of electric vehicle

Zásady pro vypracování:

- Seznamte se s problematikou zabezpečení vozidel.
- Seznamte se s systémy pro sledování a vyhledávání odcizených vozidel.
- Popište principy snímačů a zařízení používaných a použitelných pro zabezpečení vozidla (karty, otisky prstů, centrální zamykání, alarmy).
- S ohledem na potřeby nabíjení elektromobilu navrhněte řešení přístupu do prototypového elektromobilu a jeho zabezpečení proti neoprávněnému užití.

Seznam doporučené odborné literatury:

ROK ZABEZPEČENÍ VOZIDEL (PROJEKT)., ČR. Policie, ČR. Ministerstvo vnitra. Rok zabezpečení vozidel: jak ochránit svůj automobil. Česká republika: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. ISBN 8025487830, 9788025487839.
HRUŠKA, F. 2002. Technické prostředky automatizace III (Senzory, jejich principy a funkce). 1. vydání. Zlín: Vydavatelství UTB, 2002. 118 s. ISBN 80-7318-053-7.
ĎAĎO, S. – KREIDL, M. 1996. Senzory a měřicí obvody. 1. vydání. Praha: Vydavatelství ČVUT, 1996. 315 s. ISBN 80-01-02057-6.
ZHANG, Yan and Paris KITSOS. Security in RFID and Sensor Networks. 1st. USA: Auerbach Publications Boston, 2009. ISBN 1420068407, 9781420068405.
Tobin D. How hi-tech thieves are defeating keyless car security system. [online] Driving.co.uk. 3rd November 2014 Dostupné z: <http://www.driving.co.uk/news/no-car-is-safe-how-hi-tech-thieves-are-defeating-sophisticated-security-systems/>.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Martin Juránek, Ph.D.**

Datum zadání: 28.11.2014
Datum odevzdání: 30.04.2015


doc. Ing. Petr Tomčík, Ph.D.
*vedoucí katedry*

prof. Ing. Jana Dobrovská, CSc.
*děkanka fakulty*

# Zásady pro vypracování bakalářské práce

## I.

Bakalářskou prací (dále jen BP) se ověřují vědomosti a dovednosti, které student získal během studia, a jeho schopnosti využívat je při řešení teoretických i praktických problémů.

## II.

Uspořádání bakalářské práce:

1. Titulní list
2. Originál zadání BP
3. Zásady pro vypracování BP
4. Prohlášení + místopřísežné prohlášení
5. Abstrakt + klíčová slova česky a anglicky
6. Obsah BP
7. Textová část BP
8. Seznam použité literatury
9. Přílohy

ad 1) Titulní list je koncipován podle požadavků příslušné oborové katedry.

ad 2) Originál zadání BP obdrží student na oborové katedře.

ad 3) Tyto „Zásady pro vypracování bakalářské práce" následují za originálem zadání BP. („Zásady pro vypracování bakalářské práce" jsou ke stažení na webových stránkách fakulty).

ad 4) Prohlášení + místopřísežné prohlášení napsané na zvláštním listu (ke stažení na webových stránkách fakulty) a vlastnoručně podepsané studentem s uvedením data odevzdání BP. V případě, že BP vychází ze spolupráce s jinými právnickými a fyzickými osobami a obsahuje citlivé údaje, je na zvláštním listě vloženo prohlášení spolupracující právnické nebo fyzické osoby o souhlasu se zveřejněním BP.

ad 5) Abstrakt a klíčová slova jsou uvedena na zvláštním listu česky a anglicky v rozsahu max. 1 strany pro obě jazykové verze.

ad 6) Obsah BP se uvádí na zvláštním listu. Zahrnuje názvy všech číslovaných kapitol, podkapitol a statí textové části BP, odkaz na seznam příloh a seznam použité literatury, s uvedením příslušné stránky. Předpokládá se desetinné číslování.

ad 7) Textová část BP obvykle zahrnuje:

- Úvod, obsahující charakteristiku řešeného problému a cíle jeho řešení v souladu se zadáním BP;
- Vlastní rozpracování BP (včetně obrázků, tabulek, výpočtů) s dílčími závěry, vhodně členěné do kapitol a podkapitol podle povahy problému;
- Závěr, obsahující celkové hodnocení výsledků BP z hlediska stanoveného zadání.

BP nemusí obsahovat experimentální (aplikační) část.
BP bude zpracována v rozsahu min. 25 stran (včetně obsahu a seznamu použité literatury).
Text musí být napsán vhodným textovým editorem počítače po jedné straně bílého nelesklého papíru formátu A4 při respektování následující **doporučené** úpravy - písmo Times New Roman (nebo podobné) 12b; řádkování 1,5; okraje – horní, dolní – 2,5 cm, levý – 3 cm, pravý 2 cm. Fotografie, schémata, obrázky, tabulky musí být očíslovány a musí na

ně být v textu poukázáno. Budou zařazeny průběžně v textu, pouze je-li to nezbytně nutné, jako přílohy (viz ad 9).
Odborná terminologie práce musí odpovídat platným normám. Všechny výpočty musí být přehledně uspořádány tak, aby každý odborník byl schopen přezkoušet jejich správnost.
U vzorců, údajů a hodnot převzatých z odborné literatury nebo z praxe musí být uveden jejich pramen - u literatury citován číselným odkazem (v hranatých závorkách) na seznam použité literatury.
Nedostatky ve způsobu vyjadřování, nedostatky gramatické, neopravené chyby v textu mohou snížit klasifikaci práce.

ad 8) BP bude obsahovat alespoň 10 literárních odkazů, z toho nejméně 3 v některém ze světových jazyků.
Seznam použité literatury se píše na zvláštním listě. **Citaci literatury je nutno uvádět důsledně v souladu s ČSN ISO 690.** Na práce uvedené v seznamu použité literatury musí být uveden odkaz v textu BP.

ad 9) Přílohy budou obsahovat jen ty části (speciální výpočty, zdrojové texty programů aj.), které nelze vhodně včlenit do vlastní textové části, např. z důvodu ztráty srozumitelnosti.

## III.

Bakalářskou práci student odevzdá ve dvou knihařsky svázaných vyhotoveních, pokud katedra garantující studijní obor neurčí jiný počet. Vnější desky budou označeny takto:

nahoře: *Vysoká škola báňská - Technická univerzita Ostrava*
*Fakulta metalurgie a materiálového inženýrství*
*Katedra* . . . . . .

uprostřed: *BAKALÁŘSKÁ PRÁCE*

dole: *Rok* *Jméno a příjmení*

Kromě těchto dvou knihařsky svázaných výtisků odevzdá student kompletní práci také v elektronické formě do IS EDISON. Práce vložená v elektronické formě do IS EDISON se musí zcela shodovat s prací odevzdanou v tištěné formě.

## IV.

Nesplnění výše uvedených zásad pro vypracování bakalářské práce může být důvodem nepřijetí práce k obhajobě. O nepřijetí práce k obhajobě rozhoduje v tomto případě garant příslušného studijního oboru. Tyto zásady jsou závazné pro studenty všech studijních programů a forem bakalářského studia fakulty metalurgie a materiálového inženýrství Vysoké školy báňské – Technické univerzity Ostrava od akademického roku 2014/2015.

Ostrava 4. 11. 2014

**Prof. Ing. Jana Dobrovská, CSc.**
děkanka fakulty metalurgie a materiálového inženýrství
VŠB-TU Ostrava

# P R O H L Á Š E N Í

Prohlašuji, že

 jsem byl(a) seznámen(a) s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména §35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního (§60 – školní dílo);

 beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB – TUO) má právo nevýdělečně ke své vnitřní potřebě bakalářskou práci užít (§35 odst. 3);

 souhlasím s tím, že bakalářská práce bude archivována v elektronické formě v databázi Ústřední knihovny VŠB – TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;

 bylo sjednáno, že s VŠB – TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu §12 odst. 4 autorského zákona;

 bylo sjednáno, že užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB – TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB – TUO na vytvoření díla vynaloženy (až do jejich skutečné výše);

 beru na vědomí, že odevzdáním své bakalářské práce souhlasím s jejím zveřejněním podle zákona č. 111/1998Sb., o vysokých školách a o změně a doplnění dalších zákonů (Zákon o vysokých školách) bez ohledu na výsledek její obhajoby.

**Místopřísežně prohlašuji, že jsem celou bakalářskou práci vypracoval(a) samostatně.**

V Ostravě . . . . . .  . . . . . .
podpis (jméno a příjmení studenta)

# Anotace

Bakalářská práce osvětluje problematiku zabezpečení, přístupu a aktivaci elektromobilu. V teoretické části jsou popsány možnosti mechanického i elektronického zabezpečení vozidla, dálkového ovládání centrálního zamykání a aktivace vozu pomocí bezkontaktních technologií, nebo biometrických snímačů. Práce dále obsahuje návrh zabezpečení elektromobilu SCX s použitím různých technologií z hlediska aktivace vozu. V praktické části je realizace zabezpečení podle návrhu s použitím technologie RFID pro aktivaci vozu.

Klíčová slova: Elektromobil, zabezpečení proti odcizení, mechanické zabezpečení, keyless, alarm, biometrie, bezkontaktní čtení

# Annotation

Bachelor thesis explains the issue of security, access and activate the electric vehicle. The theoretical part describes the possibilities of mechanical and electronic vehicle security, remote control central locking and activating the vehicle with contactless technology, and biometric sensors. Bachelor thesis also include security draft electric vehicle SCX with using of different technology in terms of activation of the vehicle. The practical part include realization of security by draft with using RFID for activating the vehicle.

Key words: Elektric vehicle, security against theft, mechanical security system, keyless, alarm, biometrics, contactless reading

## Poděkování

Tímto bych chtěl poděkovat svému vedoucímu bakalářské práce Ing. Martinu Juránkovi, Ph.D. za odborné vedení, cenné rady při zpracování a pomoc při realizaci zabezpečení.

# Obsah

**1 Mechanické zabezpečení vozidla ..... 10**

1.1 Zámek volantu ..... 10
1.2 Elektromechanický zámek řadicí páky ..... 11

**2 Centrální zamykání ..... 14**

2.1 Dálkové ovládání centrálního zamykání ..... 14

**3 Keyless systém ..... 16**

**4 Imobilizér ..... 18**

4.1 Přídavný imobilizér ..... 19

**5 Autoalarmy ..... 20**

5.1 Jednocestné ..... 21
5.2 Dvoucestné (pagerové) ..... 21
5.3 GSM/GPS alarm ..... 22

**6 Sledování a vyhledávání vozidel ..... 24**

6.1 GSM/GPS lokátor ..... 24
6.2 Rádiové vyhledávání vozidla ..... 24
6.3 Radiové a GSM/GPS vyhledávání vozidla ..... 25

**7 Bezkontaktní čtení RFID ..... 27**

7.1 RFID čipy (tagy) ..... 27
7.2 RFID snímače (čtečky) ..... 29

**8 Bezkontaktní čtení NFC ..... 31**

8.1 Pasivní NFC zařízení ..... 31
8.2 Aktivní NFC zařízení ..... 32

**9 Biometrické skenery ..... 33**

9.1 Skenování otisku prstů ..... 33
9.2 Skenování celé ruky ..... 35
9.3 Skenování tváře ..... 37
9.4 Skenování oka ..... 39

**10 Návrh zabezpečení pro elektromobil SCX ..... 41**

10.1 Elektromobil StudentCar model SCX ..... 41
10.2 Bez klíčové zapalování ..... 42
10.3 Dálkové centrální zamykání ..... 45
10.4 Návrh algoritmu ..... 45

**11 Realizace návrhu zabezpečení pro elektromobil SCX ..... 47**

11.1 Instalace dálkového ovládání ..... 47
11.2 Instalace RFID čtečky ..... 48

**12 Závěr ..... 53**

**13 Seznam použité literatury ..... 55**

# Úvod

Smyslem této práce je seznámit se s problematikou zabezpečeníautomobilu, systémy pro sledování a vyhledávání odcizených vozidel a systémů použitelných pro zabezpečení, nebo aktivaci vozu. Objasnit jak tyto systémy fungují, uvést jaké jsou nové trendy v zabezpečení a zhodnotit jejich výhody, nevýhody a možnosti překonání. Navrhnout optimální zabezpečení pro elektromobil s ohledem na spotřebu elektrické energie a bezpečnost. Navrhnutý přístup do elektromobilu by měl být jednoduchý, intuitivní, ale zároveň bezpečný.

První kapitoly obsahují přehled běžného zabezpečení vozu, počínaje mechanickým zabezpečením až po alarmy, či vyhledávání odcizených vozidel. Zbylé kapitoly teoretické části popisují bezkontaktní čtečky a biometrické skenery, které by se mohly použít pro aktivaci vozu. Především kapitoly bezkontaktního čtení a biometrických skenerů se ubírají neobvyklým směrem v oblasti zabezpečení vozidla, a proto jsem se jim také věnoval v rámci návrhu zabezpečení pro elektromobil.

Praktická část obsahuje návrhzabezpečení a aktivace vozu pro konkrétní elektromobil z projektu StudentCar a to pro model SCX, kde se návrh také realizoval. SCX je sportovní elektromobil s nadčasovým designem a vyspělou technologií. Proto i samotný návrh byl směřován netradičními systémy a moderními technologiemi, které by ještě více podtrhovaly výjimečnost tohoto vozu.


**Obrázek 1***Elektromobil StudentCar model SCX* [1]

# 1 Mechanické zabezpečení vozidla

Při použití mechanického zabezpečení vozidla je hlavní funkcí znemožnit zloději odcizit automobil, většinou se jedná o zablokování hlavních části vozidla (volant, řadící páka, kolo) bez kterých nejde manipulovat s vozidlem.

Mechanické zabezpečení vozidla využívá buď bezpečnostní prvky pevně spojené s karoserií, nebo přenosné prvky. Mezi pevné mechanické prvky patří např. zámek řadicí páky. Mezi přenosné potom můžeme zařadit zámek pedálů, nebo botičku na kolo vozidla.

## 1.1 Zámek volantu

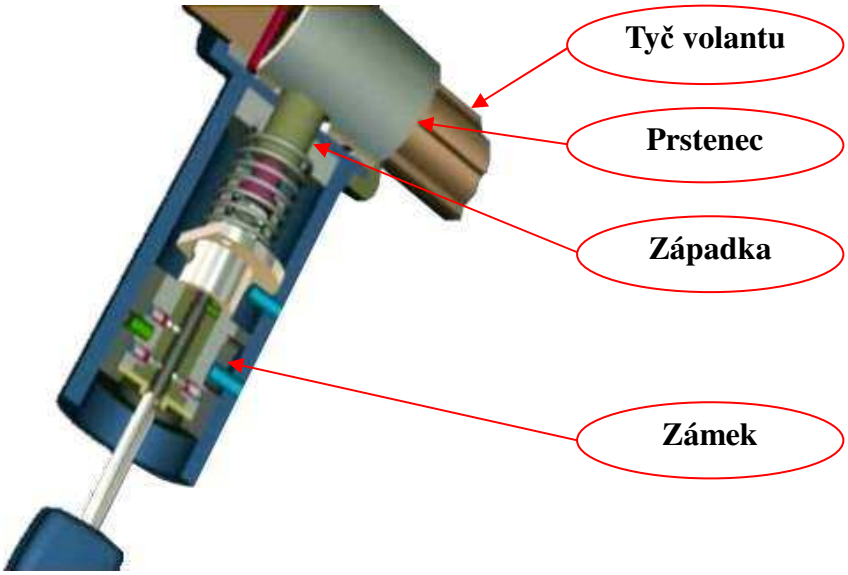
Mezi obě skupiny bezpečnostních prvků patří zámek volantu. Pákový zámek volantu, který byl donedávna jediný způsob jak zamknout volant, patří mezi přenosné mechanické prvky vizobrázek 2. Nyní je na trhu řada zámků volantu, kteréjsou pevně zabudované do sloupku řízení, tedy jsou pevně spojeny s karoserií vozidla. Na obrázku 3 můžeme vidět zástupce těchto zámků Zederlock. [2]

**Obrázek 2***Pákový zámek volantu* [3]

**Obrázek 3***Zámek volantu Zederlock* [4]

**Princip:**Zederlock zabraňuje otáčení volantu a tedy i manipulaci s automobilem, ať už v nastartovaném stavu, nebo jako tažený vůz. Montáž se provádí na pevno přímo na řídící tyč volantu. Po zamknutí nelze vůbec točit s volantem, zámek odolá tlaku šesti tun, což znemožňuje použití i pneumatických kleští.

Při zamčení vysune zámek masivní západku, která se zasune do otvoru prstence. Hrubý kovový prstenec je nejčastěji navařen na řídící tyč volantu viz obrázek 4. Specifický je také klíč, který je kulatý dutý a nemá žádné boční výstupky. Není tedy možné překonat zámek pomocí tzv. trhačů. Celý systém se navrhoval a vyráběl ve Srbsku, kde se na tom podíleli profesionální zloději, což vypovídá o jeho kvalitě vůči překonání.[4]




**Obrázek 4***Zámek volantu Zederlock*[4]

**Možnost překonání:** V případě pákového zámku volantu, který není pevně spojen s karoserií, lze volant odmontovat i s pákovým mechanismem a namontovat volant jiný. Při použití zámků pevně spojených s karoserií je překonání velmi obtížné především časově, možná i díky tomu jsou některé zámky nepřekonatelné.

## 1.2 Elektromechanický zámek řadicí páky

Pro náročnější uživatele vyvinula společnost CONSTRUCT poloautomatické zamykání řadicí páky tzv. Construct Savetronic. Systém pracuje na elektromechanickém principu. Celý systém řídí řídicí jednotka, která dává pokyn k zablokování volantu po vytažení klíče ze zapalování. Odblokování systému dochází po přiložení bezkontaktního čipu na dané místo v interiéru vozidla, toto místo může být označeno vizobrázek 5. [5]

**Princip:** Zámek funguje automaticky, k uzamčení řadícího mechanismu dochází po zařazení zpátečky a vytáhnutí klíčku ze zapalování. K odemčení dojde při identifikací čipem, který musí řidič přiložit na určité místo v interiéru. Identifikační modul načte čip a odemkne zámek. Mechanickou část zámku tvoří masivní kostra, která je pevně spojena s karoserií pomocí bezpečnostních trhacích šroubů. [5]

**Obrázek 5***Elektromechanický zámek řadící páky* [6]

**Možnost překonání:** Systém je odolný vůči extrémnímu počasí, odolává teplotám od mínus 40 do 120°C. Je odolný proti tepelným i chemickým vlivům, nekřehne ani po podchlazení tekutým dusíkem. Celý systém je uchycen bezpečnostními trhacími šrouby.Díky těmto parametrům je téměř nemožné tento systém překonat.

**Mechanické zabezpečení**

**Výhody:** Výhodou mechanického zabezpečení vozidla může být poměrně jednoduchá montáž, především u přenosných prvků. Také se nic nenapojuje na elektrické obvody automobilu, což znemožňuje systém eliminovat např. odpojením akumulátoru a také nedochází k jeho vybíjení.

**Nevýhody:** Mechanické zabezpečení funguje jako ochrana před odcizením vozidla, nikoliv před vykradením vozidla. Ve většině případů není mechanické zabezpečení kontrolováno a řízeno elektronikou, což znamená, že uživatel musí neustále myslet na uzamčení svého automobilu.

**Cenová dostupnost:** -Blokování volantu Block Shaft (od 9.000kč)
-Zámek řadící páky Construct (7.000kč)
-Zámek řadící páky Defend lock (6.500kč)

**Použití pro SCX:**Použití mechanického zabezpečení u modelu SCX nemá příliš velký význam, protože použití nejčastějšího a také nejkomfortnějšího systému, tedy zámku řadicí páky, nelze použít z důvodu, že zde je řadicí páka pouze elektronický volič. Ostatní mechanické zabezpečovací systémy nejsou příliš vhodné a komfortní pro sportovní nadčasový vůz.

# 2 Centrální zamykání

Centrální zamykání je sada motorků, které se montují do jednotlivých zámků dveří automobilu. Umožňuje řidiči zamknout, nebo odemknout všechny dveře vozidla najednou a to buď dálkovým ovladačem, nebo klíčem. Dnes už je centrální zamykání rozšířeno o individuální odemykání např. pátých dveří (kufru), nebo pouze řidičových dveří a to z důvodu bezpečnosti osob, nebo zavazadel ve vozidle. Dále může být řízeno dovírání oken, uzamykání víčka nádrže, nebo kapoty. Novější automobily mají také funkci automatického zamykání dveří po rozjetí vozidla a to buď po zařazení určitého rychlostního stupně, nebo dosažení určité rychlosti. [7]

**Obrázek 6***Sada dálkového centrálního zamykání* [7]

## 2.1 Dálkové ovládání centrálního zamykání

Dálkové ovládání je dnes samozřejmostí u nového vozu, nejčastěji je dálkový ovladač zakomponovaný společně s klíčem do zapalování vizobrázek 7. Jiné značky mají svůj vlastní designe klíče, například Renault má místo klíče kartu, kterou se aktivuje zapalování, na kartě je i dálkové ovládání a v kartě uložený nouzový klíč vizobrázek 8. Některé automobilky jako Ford mají bezklíčový přístup tzv. keyless systém.

**Obrázek 7***Dálkový ovladač s klíčem* [8]


**Obrázek 8***Přístupová karta Renault* [9]

**Typy kódování dálkového ovladače:**

Pevný kód: dálkový ovladač má stále stejný kód, který je nastaven z výroby. Tento typ kódu jde zkopírovat pomocí čtečky a později ho použít pro odemčení vozidla.

Plovoucí kód: dálkový ovladač mění svůj kód při každém stisknutí tlačítka. V tomto případě se jedná o ochranu proti naskenování kódu dálkového ovladače. Řídicí jednotka nepřijme stejný kód dvakrát po sobě.

Plovoucí kód & Antiscan: tento typ dálkového ovladače má plovoucí kód a k tomu funkci antiscan. Antiscan je ochrana proti útoku zařízení, které se snaží odemknout automobil pomocí milionů kombinací kódů. Pokud jednotka pozná v krátkém časovém úseku více kódů, zablokuje odemčení automobilu po určitou dobu. Odblokování probíhá automaticky po uplynutí dané doby, nebo po nouzovém odblokování.

**Možnost překonání:** Uvádí se mnoho možností od těch nedestruktivních, jako vyháčkování zámku přes izolaci, vyrušení signálu uzamknutí vozidla během zamykání automobilu dálkovým ovladačem, naskenování kódu až po destruktivní jako vypáčení zámku. Vše závisí na typu centrálního zamykání a na typu automobilu.

**Centrální zamykání:**

**Výhody:** Vysoký komfort pro odemykání vozidla, zvlášť s použitím dálkového ovladače.

**Nevýhody:**Vybíjení baterií v dálkovém ovladači. Především u levnějších dálkových ovladačů, nebo u koncernových automobilů možnost odemčení více automobilů pomocí jednoho ovladače.

**Cenová dostupnost:** -Centrální zamykání Keetec (3.500-4.000kč)

-Neznačkové centrální zamykání (do 1.000kč)

**Použití pro SCX:** Pro model SCX je použito dálkové centrální zamykání s plovoucím kódem.

# 3 Keyless systém

Keyless systém umožňuje řidiči bezklíčové otevírání a startování vozu. Stačí mnít klíč u sebe a pouhým přiblížením na danou vzdálenost k vozidlu (většinou okolo 1,5m kolem vozidla) se automobil sám odemkne. Poté stačí zatáhnutím kliky dveří, nebo kufru otevřít. Motor startuje pouhým stisknutím tlačítka start na palubní desce, stačí mnít u sebe klíč vizobrázek 9. Zamykání probíhá dotčením se mikrospínače umístěného na všech klikách dveří. Když zůstane klíč uvnitř automobilu systém to díky směrovým senzorům pozná a nedovolí auto uzamknout. Pokud zůstanou dveře po odemknutí 30 sekund zavřené systém opět automobil uzamkne.

Keyless ovladač má tlačítka pro dálkové ovládání, nebo i zapouzdřený klíč pro případ, že by například keyless systém nefungoval, nebo ovladač měl vybitou baterii.

Nejnovější keyless systémy mají funkci rozpoznávání řidiče, kdy si pamatuje nastavení sedadla, nebo klimatizace a to díky tomu, že každý z uživatelů má svůj vlastní "klíč". Když tedy přijde k autu, všechno se nastaví podle konkrétního uživatele. [10,11]


**Obrázek 9** *Bezkontaktní klíč (Keyless)* [12]

**Možnost překonání:**Na trhu je zařízení s názvem Q-key vizobrázek 10, které lze zakoupit přes internet. Toto zařízení dokáže odemknout, dokonce i nastartovat automobil bez jakéhokoliv poškození a to v ideálním případě až na vzdálenost 400 metrů. Celý proces trvá přibližně 30 sekund.

Toto zařízení se skládá ze dvou modulů čtečka a vysílačka, je teda zapotřebí dvou lidí. Jeden se musí dostat s čtečkou do těsné blízkosti klíče, tedy například pozoruje majitele automobilu v obchodě, načte kód klíče a pošle ho do vysílače druhému člověku, který stojí u auta. Ten už poté pomocí vysílače a načteného kódu může odemknout a nastartovat automobil.

Bránit se proti tomuto způsobu odcizení je téměř nemožné snad jen vyjmutí baterek z ovladače, což je samozřejmě proti logice celého systému, který má být co nejpohodlnější. Prozatím se zdá být jedinou variantou namontovat si do vozidla kvalitní vyhledávací zařízení, které ovšem nezabrání potencionálním zlodějům automobil odcizit.[13]

**Obrázek 10** *Q-key system* [14]

**Keyless systém:**

**Výhody:** Maximální komfort pro řidiče, vždy má volné obě ruce a nemusí při každém odemykání a startování hledat klíč od vozu.

**Nevýhody:**Možnost odemčení vozidla, ikdyž majitel jen projde kolem. Možnost odcizení vozu pomocí Q-key klíče.

**Cenová dostupnost:** -Bezdotykové dálkové centrální zamykání Keetec (1.200kč)
-PKE (Passive Keyless Entry)bezdotykové dálkové ovládání a startování vozidla pro VW, Škoda, Seat (9.000kč)
-SPY autoalarm s PKE bezdotykovým dálkovým ovládáním (2000kč)
-Dvoucestný autoalarm Magicar M1090 CAN BUS bezdotykové dálkové ovládání a startování vozidla (8.000kč)

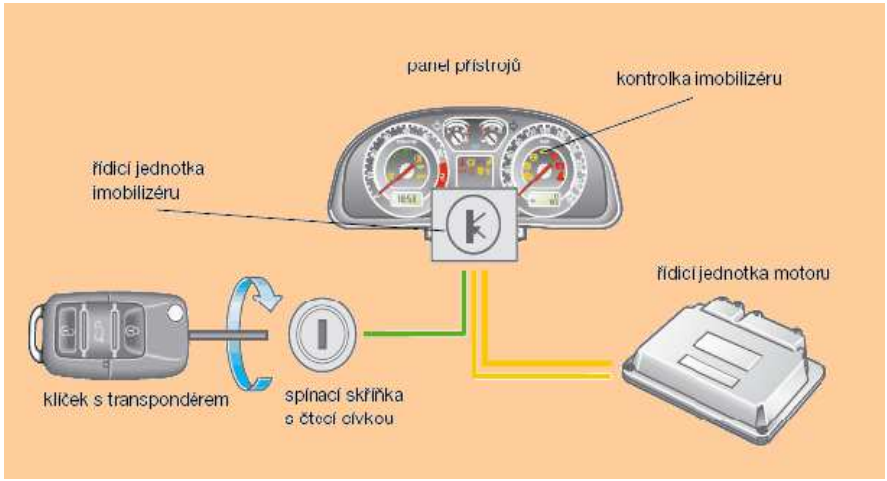
**Použití pro SCX:**Keyless je praktické a komfortní odemykání a startování pro moderní elektrický vůz. Avšak pro zvýšení zabezpečení vozu, chce systém upravit a převzít pouze myšlenku tohoto systému v podobě identifikace uživatele a bez klíčového startování.

# 4 Imobilizér

Imobilizér je elektronické zařízení integrované v automobilu většinou už z výroby. Brání nastartování motoru, pokud není ve spínací skříňce vložený správný klíč. V opačném případě imobilizér zabraňuje nastartování vozu.

**Princip:**Klíč obsahuje zakomponovaný čip s vlastním kódem, který se snímá ve spínací skříňce a dále jej posílá do řídící jednotky, která ho porovnává. Pokud tento kód nesouhlasí, řídící jednotka zabraňuje nastartování motoru a to buď odpojením přívodu paliva, nebo odpojením zapalování či jiného elektrického obvodu nutného pro nastartování.

Nevýhodou továrních imobilizérů je možnost výměny řídící jednotky (dále jen ŘJ) automobilu za jednotku z jiného vozu s vlastním klíčem. Poté může zloděj s automobilem bez problémů odjed. Zloděj si ovšem musí při krádeži vzít ŘJ s sebou a to ze stejného vozu. Samotná výměna ŘJ něco málo potrvá, ale zkušený zloděj to může zvládnout v řádech 10 sekund až minut. Záleží dle typu vozu, respektive umístění ŘJ. Proto je dnes velmi rozšířené zabezpečení kapoty vozidla, v případě, že ŘJje umístěna v motorovém prostoru.




**Obrázek 11** *Schéma zapojení imobilizéru* [15]

## 4.1 Přídavný imobilizér

Vyššího zabezpečení můžeme dosáhnout instalací dalšího imobilizéru, který se zapojuje na nezávislé okruhy elektrického systému vozidla, v tomto případě už nebude stačit vyměnit řídící jednotku, ale dekódovat i druhý imobilizér. V případě připojení druhého imobilizéru se výrazně zvýší bezpečnost vozu. Nastartování a následné odcizení se stává téměř nemožné. [16]


**Obrázek 12** *Přídavný imobilizér ATC 100/3* [16]

**Možnost překonání:**U prvních imobilizérů bylkód pořád stejný, takže šel kód pomocí čtečky zkopírovat a imobilizér tak obejít. Novější typy imobilizérů mají však plovoucí kódy, které se při každém nastartování změní, což výrazně snížilo šanci tento imobilizér obejit, přesto je tady možnost vyměnit celou řídící jednotku, kterou si pachatel s sebou vezme při krádeži. Pro maximální bezpečnost proti obejití je namontování přídavného imobilizéru, který by musel zloděj dekódovat.[16]

**Imobilizér:**

**Výhody:** Imobilizéry, především přídavné, značně komplikují zloději nastartování vozidla.

**Nevýhody:** V případě továrních imobilizérů, možnost zneškodnění výměnou řídící jednotky vozidla.

**Cenová dostupnost:** -Přídavný imobilizér ATC 100/3 (3.800kč)

-Přídavný imobilizér M3K (4.200kč)

**Použití pro SCX:** Použití imobilizéru proSCX v podobě čipu zakomponovaném v klíči je nemožné, neboť SCX nemá spínací skříňku na klíč. Systém podobný imobilizéru může být použitpro aktivaci vozu.

# 5 Autoalarmy

Autoalarmy používáme nejčastěji jako poplašné zařízení, kdy při násilném vstupu do vozidla, nebo jeho manipulací, se spustí siréna, nebo klakson společně s výstražnými světly, což dokonale upoutá pozornost všech lidí okolo a tedy vyplaší zloděje. Modernější a dražší alarmy jsou vybaveny pagerem, přes který komunikují s uživatelem a sdělují mu informace o voze. Trochu jinou kategorii tvoří GSM/GPS alarmy, které spíše slouží k vyhledávání vozu. Tyto alarmy využívají GSM sítě pomocí předplacených SIM karet, přes které komunikují s uživatelem a díky GPS mohou zasílat souřadnice vozu.

**Alarm může obsahovat různá čidla:**

Otřesové čidlo:spustí alarm při otřesu, neboli pohybu vozidla nad určitou přípustnou hodnotu, kterou si buď uživatel nastaví sám, nebo je nastavena výrobcem. Citlivost se musí nastavit tak, aby alarm nespustil např. při silném větru.

Polohové (náklonové) čidlo:hlídá, zda je vůz ve stejné vodorovné poloze od aktivace alarmu. Tento druh čidla se často kombinuje s ostatními, pro případ že by se někdo snažil automobil odtáhnout a tedy by musel s autem najet na odtahové vozidlo, při tom by došlo k náklonu, který by zpustil alarm.

Detektor tříštění skla: pracuje na principu snímaní zvuku o vlnové délce a tlaku, který právě odpovídá tříštění skla.

Ultrazvukové čidlo:jedná se od dva malé detektory, kdy jeden funguje jako vysílač, druhý jako přijímač ultrazvukového signálu. Při zastínění tohoto signálu dojde ke změně ultrazvukové energie, která se mění po odrazu určité překážky. Při této změně dochází k poplachu. Nevýhodou tohoto typu čidel je vysoká spotřeba elektrické energie.

Mikrovlnné čidlo: pracuje na principu mikrovlnného záření, které se vysílá a zároveň přijímá z čidla. Pozoruje změnu intenzity tohoto záření. Stejně jako u ultrazvukového čidla je vyšší spotřeba elektrické energie, protože čidlo musí neustále vysílat nějaký typ záření.

PIR (infračervené) čidlo: zde může být použitá infračervená závora, která se skládá s vysílače a přijímače infračerveného záření. Nebo může být použito PIR čidlo, které snímá infračervené záření o vlnové délce, které odpovídá člověku.

Autoalarmy můžeme rozdělit podle toho, jak informují uživatele o probíhající krádeži, či odcizení vozidla na: a)jednocestné

b)dvoucestné

c)GSM/GPS

## 5.1 Jednocestné

Jde o základní zabezpečení vozidla, kdy při vloupání začne automobil houkat a blikat výstražnými světly, aby co nejlépe upoutal pozornost okolí a tím vyplašil zloděje. Výhodou jednocestných autoalarmu jsou nižší pořizovací náklady.

Jednocestný autoalarm se nejčastěji skládá z řídicí jednotky, sirény, indikační led diody, dálkového ovladače, čidel, kabeláže a instalačního materiálu vizobrázek 13.

**Obrázek 13** J*ednocestný autoalarm* [17]

## 5.2 Dvoucestné (pagerové)

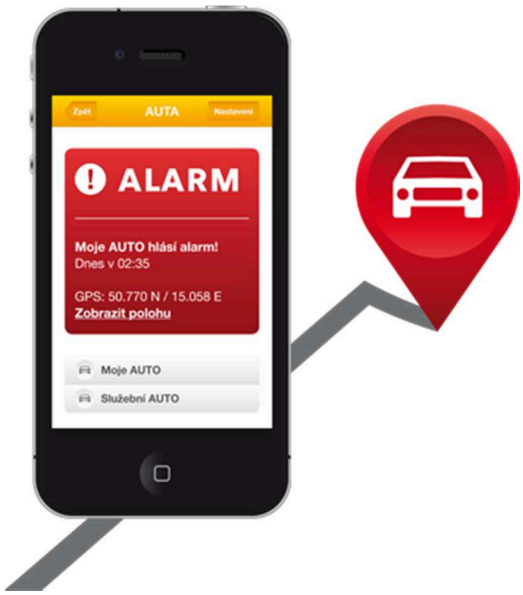
Jsou zabezpečovací systémy, které při násilném vstupu do vozidla, nebo jeho manipulací vysílají majiteli vozu informace na pager. Pager mívá dosah až 2km ve volném prostranství od vozidla, může mít také funkci dálkového startu, dovíraní oken, nebo otevíraní kufru. Pokud je vybaven displayem, může také zobrazovat informace o vozidlu, např. signalizace zatažení ruční brzdy, otevřených dveří, nebo příčinu spuštění alarmu. [18]


**Obrázek 14** *Pager dvoucestného autoalarmu* [18]

## 5.3 GSM/GPS alarm

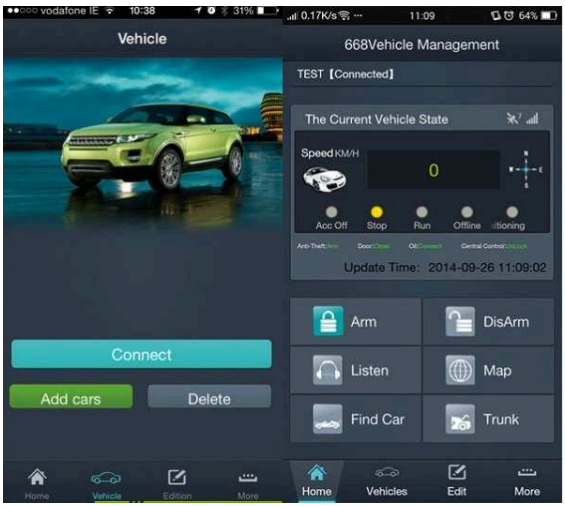
Je zabezpečovací systém vybavený bezdrátovým přenosem informací pomocí sítě GSM, v kombinaci s GPS může zasílat zeměpisné souřadnice automobilu. Při násilném vstupu do vozidla, nebo jeho manipulací, může alarm pomocí sítě GSM zaslat SMS zprávu majiteli, nebo bezpečnostní agentuře s informacemi, že se někdo snaží dostat do auta a to včetně zeměpisných souřadnic, kde se právě automobil nachází, viz obrázek 15. To může např. bezpečnostní agentuře pomoc pro rychlý příjezd na místo.

Alarmy GSM, které jsou vybavené GPS signálem,mohou za jízdy zapisovat informace o poloze vozidla, to lze využit při vyhledávání odcizeného vozidla, nebo pro sledování firemního vozu a tvorbu knihy jízd. [19]

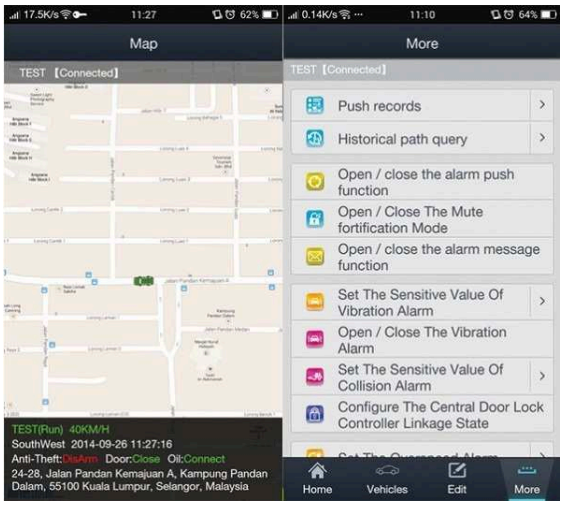



**Obrázek 15** *SMS zpráva alarmu* [19]

Novinkou mezi GSM/GPS alarmy je komunikace s automobilem pomocí telefonu, díky kterému můžeme auto odemknout, zamknout, vyhledat, nastartovat či dokonce telefonovat s osobou ve voze. Na obrázku 16 lze vidět připojení k vozu pomocí chytrého telefonu a základní menu, kde nalezneme odemknutí, zamknutí vozu, vyhledávání vozu atd. Na obrázku 17 je zobrazena komunikace vozu s chytrým telefonem a lokalizace automobilu na mapě.




**Obrázek 16** *Aplikace GSM/GPS alarmu, dálkové odemykání vozu* [20]




**Obrázek 17** *Aplikace GSM/GPS alarmu, lokalizace automobilu a komunikace* [20]

**Možnost překonání:**Nevýhodou GSM/GPS alarmu může být odcizení vozidla pomocí rušičky těchto signálu, které lze zakoupit na internetu.

**Autoalarmy:**

**Výhody:**Alarmy jednocestné můžou vyplašit, nebo odradit potencionální zloděje. Dvoucestné neboli pagerové a GSM/GPS alarmy posílají informace o vozidle přímo majiteli, v případě GSM/GPS mohou pomoci při vyhledávání odcizeného vozidla.

**Nevýhody:**U alarmu využívajících aktivní čidla je velká spotřeba elektrické energie, kdy při delší době odstaveného vozidla může dojít k vybití akumulátoru. U alarmu GSM/GPS jsou vyšší pořizovací náklady.

**Cenová dostupnost:** Alarm jednocestný Keetec (4.500kč)
Alarm jednocestný Jablotron (5.500kč)
Pagerové Keetec (6.500-7.500kč)
Pagerové Magicar (8.000-10.000kč)
GSM/GPS Jablotron (12.500kč)

**Použití pro SCX:** Nejlepší variantou pro SCX by byl GSM/GPS alarm, který by komunikoval s vozem pomocí telefonu.

# 6 Sledování a vyhledávání vozidel

Sledovat, nebo vyhledat vozidlo můžeme pomocí rádiového signálu, GSM/GPS signálu, nebo jejich kombinací. Nejčastější variantou jsou GSM/GPS lokátory, které díky své nízké pořizovací ceně jsou snadným zabezpečením vozu. Radiové vyhledávání se používá především u dražších vozů, kde jsou vysoké nároky na kvalitu služeb a vysokou úspěšnost, což odpovídá pořizovacím i měsíčním nákladům.

## 6.1 GSM/GPS lokátor

GSM/GPS lokátor je velmi podobný s GSM/GPS alarmem, základní funkce je stejná, komunikace přes GSM síť s možností sledování vozidla GPS signálem. Rozdíl je, že alarm je přizpůsobený k aktivaci zařízení v době, kdy auto stojí v klidu, zamčené a je nějakým způsobem narušeno, což pozná díky čidlům. Lokátor má funkcí několik, funguje i 24 hodin 7 dní v týdnu. Nejčastěji je používán jako elektronická kniha jízd a k tomu je i příslušně vybaven funkcemi, jako je sledování v reálném čase, upozornění na pohyb vozidla, odposlech interiéru, upozornění na překročení určité rychlosti, nebo vzdálení automobilu od přednastavené pozice a mnohé další. Některé lokátory mají i funkci alarmu, stejně jako GSM/GPS alarm může mít funkci elektronických knih jízd. Obě tyto zařízení jsou schopna vyhledat, nebo sledovat vůz v reálném čase. Jedná se o stejné zařízení více, či méně přizpůsobené k jednomu, nebo druhému použití.
**Možnost překonání:** Stejně jako u GSM/GPS alarmu lze vyrušit signál pomocí rušičky signálu.

## 6.2 Rádiové vyhledávání vozidla

Radiové vyhledávání probíhá přes rádiové vlny o frekvencích, které se neshodují s běžnými rádiovými frekvencemi. Provozovatelé, u nás nejznámější Sherlog, mají proto své vlastní rádiové věže, které pokrývají celou Českou republiku, viz obrázek 18. Jedná se tedy o placenou službu s měsíčním poplatkem přibližně 500kč. Vyhledávací společnosti jsou vybaveny osobními i terénními vozy, někdy dokonce leteckými prostředky. Při pronásledování ukradeného vozidla spolupracují s policií.

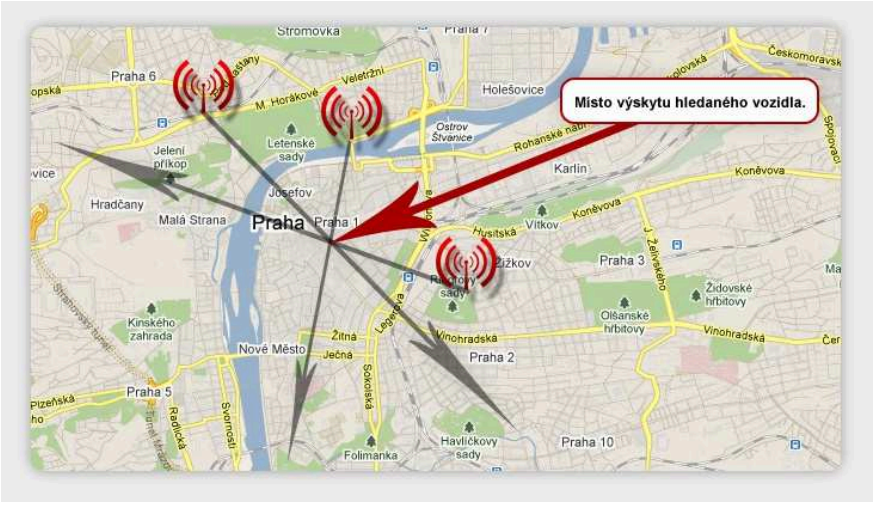
Aktivace proběhne tehdy, když se automobil rozjede a nedojde k načtení čipu podobně jako u přídavného imobilizéru. Při aktivaci, dostane operační středisko tísňový signál, který operátoři telefonátem ověřují u majitele, zda se jedná o krádež, nebo o falešný poplach. Při potvrzení krádeže se ihned rozjede pátraní a lokalizace automobilu. [21]

**Obrázek 18** *Rádiová věž Sherlog*[21]

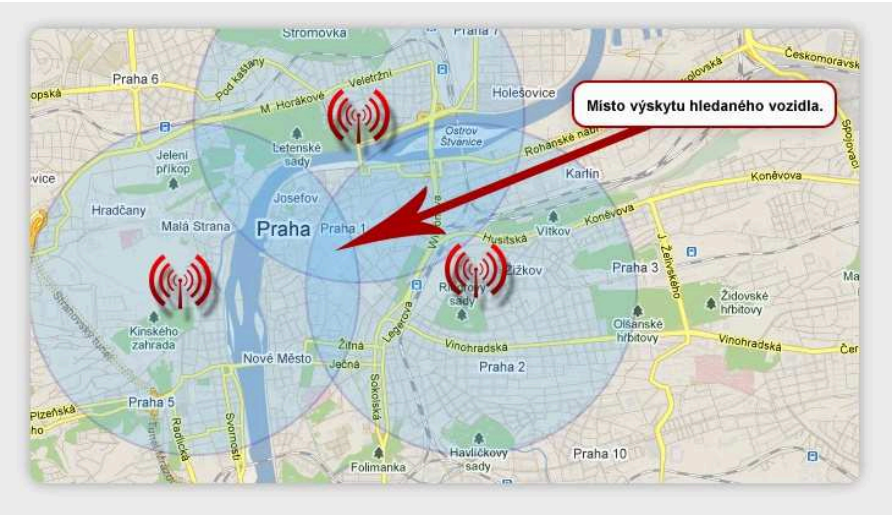
**Možnost překonání:** Sherlog udává, že jako jediný je imunní proti rušení rádiového signálu rušičkou. Je schopen vyhledat rušení vlastního signálu, čímž rušička dokonce pomáhá při hledání vozidla.

## 6.3 Radiové a GSM/GPS vyhledávání vozidla

Spojení radiového a GSM/GPS signálu je nejvyšší úrovni vyhledávání vozidel. Jedná se o spojení dvou na sobě nezávislých vyhledávacích systémech s pokrytím nejen České republiky, nebo Evropy, ale i za oceán. Aktivace systému nastane, pokud dojde k pohybu vozu bez přiložení čipu. Stejně jako u rádiového vyhledávání dojde nejdříve k telefonnímu ověření krádeže a až po ověření dojde k pátrací akci. Na obrázku 19 a 20 je ukázka lokalizace automobilu.[22]




**Obrázek 19** *Vysílání rádiového signálu*[22]




**Obrázek 20** *Lokalizace automobilu*[22]

**Možnost překonání:** Tento systém dosahuje nejvyšší bezpečnosti proti rušení signálu, u již zmíněného rádiového signálu je problém s rušením. V případě spojení dvou různých na sobě nezávislých signálů je rušení jednoho signálu nedostačující, protože druhý typ signálu stále lokalizuje automobil.

**Sledování a vyhledávání vozidel:**

**Výhody:**Většina společností provozující rádiové vyhledávání vozu garantuje vrácení automobilu do 2hodin s úspěšností až 98%.

**Nevýhody:**V případě GSM/GPS lokátoru lze signál vyrušit. Rádiové vyhledávání je finančně náročné.

**Cenová dostupnost:** GSM/GPS lokátor (od 800-15.000kč)
Radiové vyhledávání Sherlog (30.000kč vč. instalace a aktivace+měsíční paušál 500kč)

**Použití pro SCX:**Žádné z těchto vyhledávacích zařízení není potřeba, u již zmíněných alarmů by byl nejlepší GSM/GPS alarm, který už umožňuje vyhledat vůz. Pro použití rádiového vyhledávání se nejedná o příliš ohrožený typ automobilu z důvodu malosériové výroby.

# 7 Bezkontaktní čtení RFID

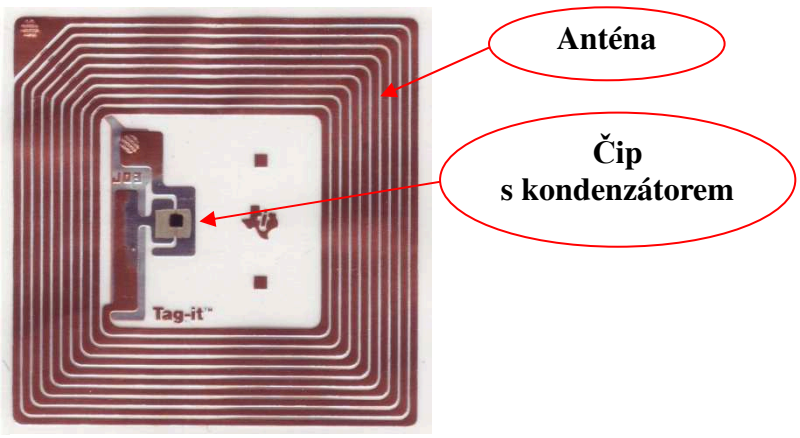
RFID (Radio Frequency Identification)- jde o bezdrátový rádio frekvenční přenos dat, při kterém nedochází ke spojení kontaktů snímače (čtečky) a identifikátoru (tagu). Tagy proto můžou být hermeticky uzavřeny v pouzdře, tudíž odolávají oxidaci, vlhkosti i prachu. Jsou tedy ideální pro provoz, navíc nepotřebují žádný zdroj energie, tu získávají ze snímače. Pokud se jedná o přístupové systémy mají čipy (tagy) nejčastější zapouzdření v podobě karet, nebo klíčenek vizobrázek 21.

V automobilovém průmyslu se můžeme setkat s RFID nejčastěji v imobilizérech, popř. alarmech, nebo pro odblokování elektromechanických zámků řadicí páky.[23]


**Obrázek 21** *Přístupové RFID čipy* [24]

## 7.1 RFID čipy (tagy)

RFID tag se skládá z čipu, kondenzátoru a antény vizobrázek 22, jeho úkolem je zachytávat impulzy vysílané komunikačním rozhraním a odpovídat na ně. RFID tagy sice nepotřebují žádný zdroj energie, ale mohou ho mít např. pro větší dosah signálu.




**Obrázek 22** *RFID tag (čip)* [25]

**Rozdělení podle zdroje energie:**

Pasivní: Nejlevnější varianta RFID čipu, díky které jsou tyto čipy nejpoužívanější. Nepotřebují žádný zdroj energie, tudíž nemohou vysílat žádné informace směrem k přijímači. Čtečka vysílá periodicky pulsy do okolí, pokud se v blízkém okolí nachází pasivní čip, dojde k nabití jeho napájecího kondenzátoru a poté čip odešle odpověď čtečce. Nejsou náročné na obsluhu a jsou odolné. Akční čtecí vzdálenost se liší podle frekvence. Velikost paměti 64-256 bits.

Aktivní: Aktivní čipy vysílají informace do okolí samy a to díky zabudované malé baterie. Díky baterii mají čipy menší odolnost proti teplotám a je nutné baterie vyměňovat, proto se používají spíše pro sledování lidí, aut, nebo zvířat. Jejich dosah je až 100m. Nevýhodou jsou vyšší pořizovací náklady.

Semiaktivní:Jedná se o pasivní čip, který nemůže vysílat. Obsahuje baterii pouze pro větší dosah signálu.

**Rozdělení podle frekvence a dosahu:**

Každý tag (čip) má od výroby svojí frekvenci nosného signálu. Od frekvence se odvíjí maximální dosah vysílaného signálu. [26]

Nízkofrekvenční (LF): - frekvence 125 a 135kHz

- dosah 0,5m
- rychlost komunikace je pomalejší
- dobré čtení přes kapaliny, částečně i přes kov

Vysokofrekvenční (HF): - frekvence 13,56MHz

- dosah 1m
- rychlost komunikace je vyšší než u LF
- čtení přes kapaliny a kov je znatelně horší než u LF

Ultravysokofrekvenční (UHF): - frekvence 865-869MHz pro Evropu a Afriku, 902-928MHz pro Ameriku, Canadu, 950-956MHz pro Japonsko a Asii.

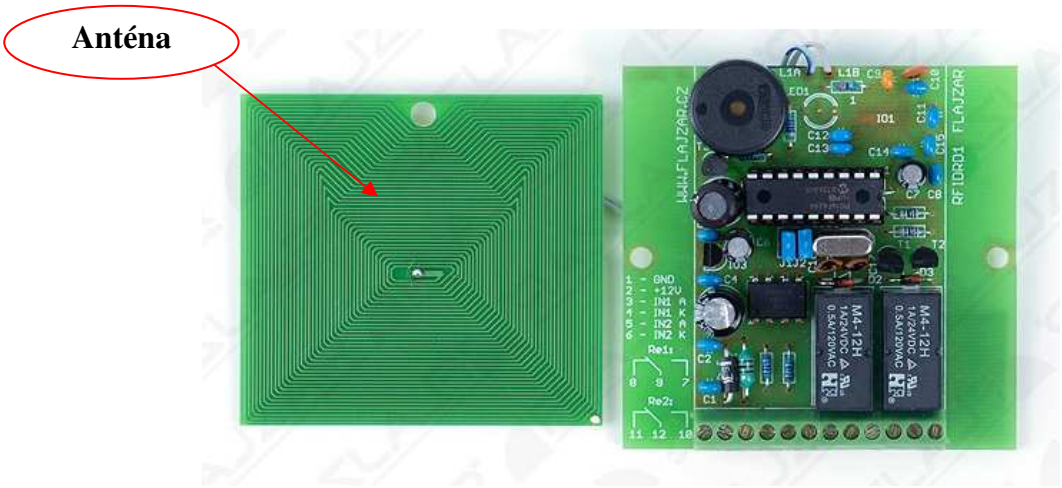
- dosah 3m
- rychlost komunikace vysoká (použití mýtné brány)
- čtení přes kapaliny vůbec, přes kov velmi omezeně

Mikrovlnné (MW): - frekvence 2,45 a 5.8GHz

- dosah 10m
- rychlost komunikace až 2MB/s
- jsou náchylné už na blízkost kapalin a kovů

## 7.2 RFID snímače (čtečky)

Čtečkaje zařízení, které dokáže zachytit vysílaný signál aktivního, nebo pasivního čipu (tagu). Pro přenos informací má čtečka anténu vizobrázek 23. Úkolem čtečky je zpracovávat obrovské množství dat získané i od více tagů ve velmi krátkém časovém úseku.




**Obrázek 23** *RFID čtečka* [27]

Čtečka může být mobilnívizobrázek 24, nebo stacionární viz obrázek 25. Stacionární se montují tam, kde tagy "chodí" za čtečkou, tedy v případě přístupových systému apod. Mobilní se používá např. ve skladech, kde se s čtečkou chodí a snímají se tagy.

**Obrázek 24***Mobilní RFID čtečka* [28]

**Obrázek 25** *Stacionární RFID čtečka* [29]

**Možnost překonání:**Největším nebezpečím je bezkontaktní čtení čipu RFID. Načtením lze získat informace, nebo biometrické údaje, které můžou sloužit jako identifikace pro přístupové systémy. To lze provádět i ze vzdálenosti deseti metrů, ikdyž technické údaje přístrojů garantují funkčnost ve vzdálenosti jen několik centimetrů, pokusy ukázaly, že čtečky dokážou přečíst čip z mnohem větší vzdálenosti.

Také je možnost hacknutí celého RFID systému pomocí zavirovaného čipu, který čtečka načte a tím natáhne virus do svého systému. Na tuto skutečnost upozornil Bruno Crispo z univerzity v Amsterdamu. Virus využívá slabá místa v systému, následně může položit celý systém. Příklad uváděl na systému v supermarketu, kde si zakoupíte zboží s RFID čipem, doma jej vyměníte za zavirovaný a zboží vrátíte do supermarketu, poté může dojí k totálnímu zhroucení celého informačního systému. [30]

**Bezkontaktní čtení RFID:**

**Výhody:** Jednoduchá konstrukce, nízké pořizovací náklady, bez potřeby zdroje elektrické energie pro tag, signál projde přes tenčí překážky.

**Nevýhody:**RFID nemá dostatečné zabezpečení.

**Cenová dostupnost:** RFID stavebnice (1000kč)

**Použití pro SCX:**Použití RFID je dobrou náhradou místo klasického klíče do zapalování. Čip může aktivovat elektromobil a zároveň může plnit funkci imobilizéru.

# 8 Bezkontaktní čtení NFC

NFC (Near Field Communication)- je bezdrátový přenos dat na krátkou vzdálenost, většinou pár milimetrů až centimetrů. NFC pracuje na frekvenci 13,56MHz. Vychází z principu RFID, jedná se pouze o novější technologii. Největším rozdílem je, že NFC může komunikovat oboustranně. Tedy, že data se mohou z čipu nejen číst, ale také do něj zapisovat. K zápisu dat má NFC tag paměť, jedná se tedy o paměťové zařízení s možností čtení bezdrátově. Stejně jako u RFID nepotřebuje zdroj elektrické energie, tu si tag bere pomocí elektromagnetického pole z aktivního NFC zařízení. Proto se také používá od roku 2011 v bezkontaktních platebních kartách.[31]

**Rozdělení podle režimu přenosu:**

Reader/writer: Jedná se o režim čtení/zápis NFC tagu. Bezpečnost tohoto přenosu není příliš vysoká, v případě použití pro platební karty se data šifrují. Čtení i zápis, ať už do čipu, nebo z něj se provádí při pasivním napájení, tedy elektromagnetickým polem čtečky. Maximální rychlost přenosu dat je 106kb/s.

Peer-to-peer: Je vzájemná výměna dat, SMS, nebo kontaktů mezi dvěmi aktivními NFC zařízeními. Každé zařízení může komunikovat oběma směry, tedy vysílat i přijímat, nikoliv však současně. Vždy může jen jedno zařízení vysílat, nebo přijímat. Maximální rychlost přenosu dat je 424kb/s.

Card emulation: Je režim, kdy aktivní NFC zařízení nahradilo pasivní NFC tag. V případě komunikace se aktivní NFC zařízení např. mobilní telefon chová jako pasivní tag např. jako vstupenka, nebo jízdenka.

## 8.1 Pasivní NFC zařízení

Pasivní NFC zařízeníje v podstatě tag, který se skládá z antény a čipu. Anténa slouží ke komunikaci. Čip se skládá z kondenzátoru, který akumuluje elektrickou energii, z paměti, ve které jsou uložená data a řídící jednotky.

NFC tag může být v podobě nálepky, karty, nebo přívěšku. Velikost tagu se odvíjí od velikosti antény, ty nejmenší mají v průměru 15mm a tloušťku desetiny milimetru.

Typů NFC tagů je spousta a liší se podle několika parametrů, jako rychlost přenosu, velikosti paměti, funkční vzdálenosti, možnosti uzamčení, nebo šifrování.

NDEF (NFC Data Exchange Format): je formát pro přenos dat mezi různými NFC zařízeními. Díky tomu jakékoliv data zapsané do NFC tagu, budou stejně čitelné i v jiném NFC zařízení.[31]

## 8.2 Aktivní NFC zařízení

Aktivní NFC zařízení jsou schopny číst i zapisovat data. Mohou tedy vysílat elektromagnetické pole pro napájení tagu. Může se tedy jednat o platební terminály, mobilní telefony podporující NFC technologii, nebo jiné čtecí zařízení.

Může také docházet k vzájemné výměně dat mezi dvěmi aktivními zařízeními, jedno tedy nahradí pasivní NFC čip. Může takto docházet k výměně dat např. mezi dvěma mobilními telefony. V jeden daný okamžik může jedno zařízení jen vysílat, nebo přijímat data. Jedná se o přenos peer-to-peer, který se nejčastěji používá při bezkontaktním placení, tedy platební terminál a mobilní telefon.[31]

**Možnost překonání:** NFC signál může být zachycen speciálním zařízením s anténou a tak načítat data, při odchytávání signálu aktivního zařízení může fungovat zařízení až na 10m, u pasivního NFC zařízení se jedná o vzdálenost do 1m, ale spíše v řádech centimetrů. Načtením například platební karty lze získat základní informace, jako jméno, číslo karty, typ a datum expirace, to stačí pro nakupování v některých internetových obchodech. Proti tomu nejsou karty chráněny, ale samotný převod informací je šifrovaný. V případě použití šifrovaného NFC tagu jako bezkontaktní přístup je tedy ohrožení minimální.

**Bezkontaktní čtení NFC:**

**Výhody:** Bez potřeby zdroje elektrické energie pro tag, možnost čtení i zápisu dat do tagu, možnost šifrování tagu.

**Nevýhody:**Vyšší pořizovací náklady u tagu s větší paměti a možnosti šifrování.

**Cenová dostupnost:** NFC modulu (od 2.000kč)

NFC karta iClass 2k bit 2000PGGMN, šifrovaný přenos dat, určený pro přístupové systémy a bezhotovostní platby (150kč)

**Použití pro SCX:**Jedná se o bezpečnější náhradu za RFID pro aktivaci vozu, navíc s možností zápisu informací.

# 9 Biometrické skenery

Biometrické technologie rozpoznávání lidí jsou nejlepším způsobem, jak identifikovat osobu. Jsou to údaje, které získáváme měřením velikosti, tvaru, nebo strukturou určitých fyziologickýchznaků části lidského těla. Většina biometrických znaků člověka jsou jedinečné a s velice vysokou pravděpodobností neexistují dva lidé, kteří by měli stejné otisky prstů, nebo stejnou sítnici oka. To ještě neznamená, že nejdou tyto rozpoznávací zařízení obejít, není to ovšem tak jednoduché, jako rozpoznat heslo, nebo napodobit podpis.

Některé biometrické skenery nelze obejít téměř vůbec, snímaní oka je na obejití jedno z nejtěžších. Oko totiž musí být "živé", prokrvené a nejlépe ve své oční jamce.

Nejpřesnější metodou je DNA, které lze získat z jakékoliv buňky těla. Na trhu se objevuje stále více nových technologii jak rozpoznat lidi s vysokou přesností a zároveň, aby systém byl jednoduchý a rychlý.

**Přesnost biometrických metod vůči jejich chybovosti:**

| | |
|---|---|
| sítnicová biometrie | 1 : 10 000 000 |
| duhovková biometrie | 1 : 130 000 |
| otisky prstů | 1 : 500 |
| geometrie ruky | 1 : 500 |
| podpis | 1 : 50 |
| hlasová identifikace | 1 : 50 |

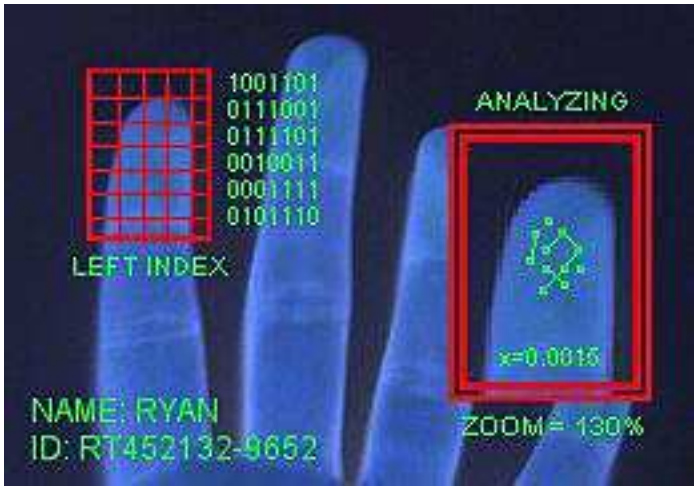
**Tabulka 1***Porovnání bezpečnosti biometrických metod*(Data převzata z WSEAS International Conference on Signal Processing, Robotics and Automation, Corfu Island, Greece, 2007)

## 9.1 Skenování otisku prstů

Donedávna byly skenery otisku prstů spíše záležitosti nadnárodních společností, nebo společností s vysokou úrovní zabezpečení a to díky vysoké pořizovací ceně těchto skeneru. Časem se díky novým technologiím podařilo snížit cenu těchto čtecích zařízení natolik, že se zpřístupnily většině uživatelů, proto se dnes už běžně používají jako docházkové systémy ve firmách. Zároveň se zvýšila rychlost mikroprocesorů a zdokonalily algoritmy pro porovnávání otisků prstů.

Systém je dokonalý v tom, že neexistují dva lidé, kteří by měli stejné otisky prstů, proto nemůže dojít k záměně otisku prstů, neboli k záměně dvou osob.[32]

**Princip:** Po přiložení prstu čtečka naskenuje otisk prstu ve vysokém rozlišení, poté pomocí výkonného procesoru vyhodnotí důležité body, kterým následně přiřadí jedinečné ID číslo.Toto ID číslo se potom porovnává s vnitřní databázi, a v případě shody ho přiřadí danému uživateli.




**Obrázek 26** *Analýza otisku prstů* [32]

**Skenovací zařízení otisku prstů**: Skenovací zařízení funguje v podstatě stejně, jako čtečka RFID, pouze místo načítaní čipů dochází ke snímání otisku prstu. Také stejně jako u RFID čteček je nutné načíst do databáze otisky prstů, u některých systému se skenují raději dva prsty, pro případ zranění, nebo velkého znečištění prstů. Typy skenovacích zařízení je spousta na obrázku 27 vlevo můžeme vidět standardní přístupový skener
a napravo je vidět stavebnice s veškerou potřebnou elektronikou.

**Obrázek 27** *Přístupová čtečka* [32, 33]

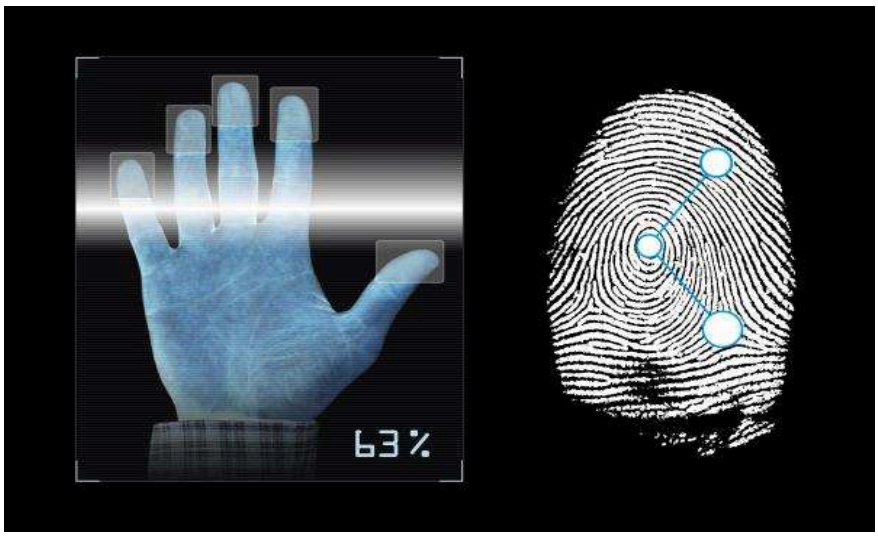
**Možnost překonání:**Možnost zrekonstruovat otisk prstů z fotografie, jednomu z členů CCC (Chaos Computer Club) se totiž údajně podařilo zrekonstruovat otisk prstu jedné německé političce z kvalitní fotografie dlaně a to za pomocí komerčního softwaru VeriFinger. Otisk prstů můžeme také získat z předmětu, kterého se uživatel uchopí.

Proto se nyní uvažuje, zdali by měly otisky prstů tvořit jediný bezpečnostní přístupový, nebo přihlašovací prvek. Některé zdroje doporučují používat otisk prstů spíše jako "přihlašovací jméno, než heslo“, nebo alespoň kombinovat otisk prstů s heslem.[34]


**Obrázek 28** *Zrekonstruovaný otisk prstu společně s fotografii hackera* [34]

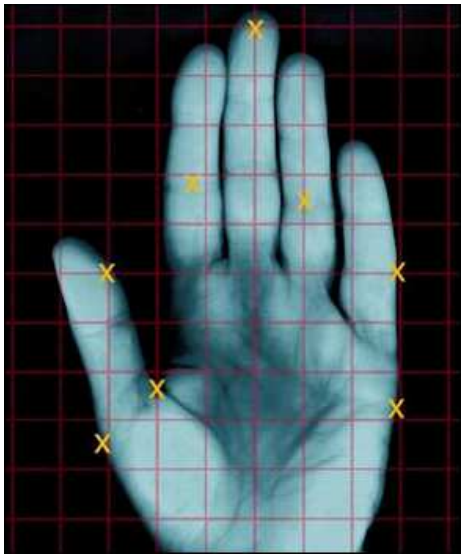
## 9.2 Skenování celé ruky

Kromě otisku prstu, může být skenovaní celé ruky, kde se porovnává kompletní geometrie ruky. Rozvržení prstů jejich délka, tloušťka, nebo tvar. Tvar ruky se ovšem s věkem mění daleko rychleji, než u ostatních biometrických části těla, které podléhají změnám s přibývajícím věkem. Tato technika není příliš rozšířená, spíše se používá jako docházkový systém.




**Obrázek 29** *Otisk celé ruky* [35]

**Princip:** Systémy mohou pracovat na různém principu na porovnávání geometrie prstů, geometrie ruky, siluety ruky, nebo dokonce analyzovat žíly. Nejprve se musí naskenovat celá ruka ve 2D, nebo 3D prostoru. Poté se porovnává délka, šířka, boční profil, nebo výstupky prstů. Stejně, jako u otisku prstů se porovnávají určité body naskenované ruky, které se vytváří na výstupu skeneru v podobě x-dimensionální fotografie vizobrázek 30.[36]



**Obrázek 30** *Fotografie ruky v x-dimensionální podobě*[37]

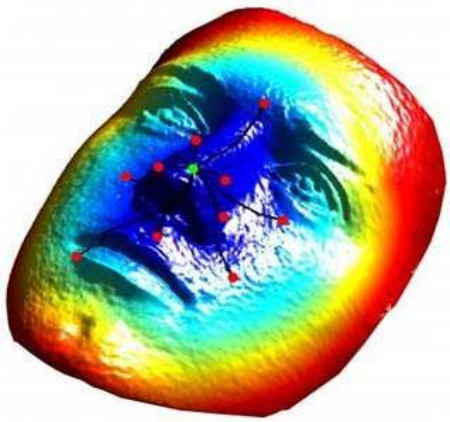
Další již zmíněnou možností snímání celé ruky je snímání žil a cév. Celý systém funguje bezdotykově, stačí dlaň pouze přiložit ke snímači, což zvyšuje hygienu pro veřejná místa. Tento systém se používá v Japonsku na universitách, v nemocnicích, nebo v platebních bankomatech. Jedná se také o velmi bezpečné snímání, protože řečiště je schované pod kůži a je těžké ho napodobit. Některé systémy navíc monitorují, zda je krev teplá a proudí.

**Princip:** Snímání dlaně, nebo hřbetu ruky se provádí pomocí nasvícení led diodami. Ty prosvítí ruku a díky propustnosti a absorpci infračerveného záření jednotlivých žil a cév se vytvoří snímek. Ten se snímá pomocí CCD kamery. Ze snímání vznikne černobílý snímek se stromovou strukturou vizobrázek 31. Dále se snímek digitalizuje a opět se porovnávají body a úhly rozmístění cév.[38]

**Obrázek 31** *Snímek řečiště*[39]

## 9.3 Skenování tváře

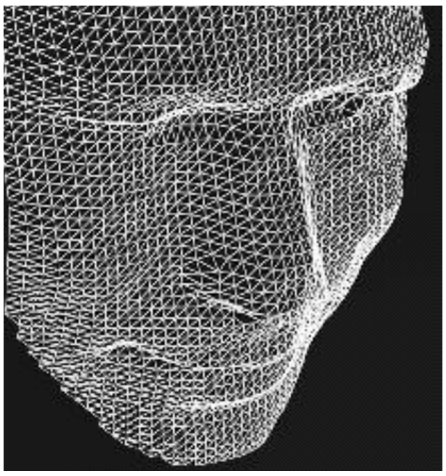
Skenování a následně rozpoznávání tváře je náročná výpočetní operace, která se díky zrychlujících se počítačů stále rozšiřuje. První známější použití se objevilo u notebooků jako přístupové zabezpečení, kdy notebook porovnával shodu tváře pomocí pořízeného snímku zabudovanou web kamerou. Rozpoznávání tváře se používá v různých programech, které spravují sbírky fotografii. Nyní se díky novějším způsobům snímání posunulo rozpoznávání tváře na profesionální použití. Díky infrakameře lze snímat i hloubku tváře, což umožňuje vytvořit trojrozměrný obraz a tím zpřesnit identifikaci.[39]



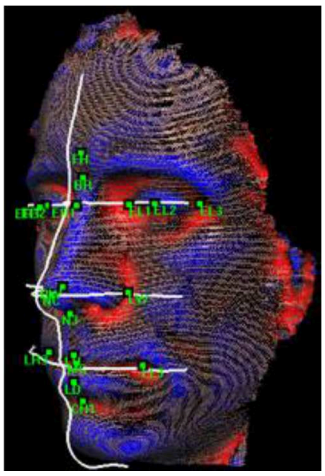
**Obrázek 32** *Trojrozměrný obraz tváře* [39]

**Princip:** Rozpoznávání tváře můžeme rozdělit do 2 způsobů, první je geometrický, zaměřuje se na rysy tváře, druhý je fotometrický, ten se zaměřuje na vzhled tváře. Pro rozpoznávání tváře jsou 3 nejznámějšími algoritmy, PCA (Principal Components Analysis) analýza hlavních částí, LDA (Linear Discriminant Analysis) lineární diskriminační analýza a EBGM (Elastic bunch graph matching) elastický srovnávací diagram.

Metoda PCA a LDA nebyly příliš dokonalé, nedokázaly identifikovat osobu se změnou osvětlení, nebo s nedokonalou pozicí tváře. EBGM metoda označí na tváři body, které se propojí a tím vytvoří souřadnicovou síť vizobrázek 33. Porovnávání probíhá pomocí filtru bodů, který porovnává body s ostatními tvářemi viz obrázek 34. [38]



**Obrázek 33***Souřadnicová síť obličeje*[38]



**Obrázek 34***Porovnávací body tváře*[38]

**3D čtečka obličejů:** Systém Broadway 3D je první přístroj na světě, který dokáže identifikovat obličej v 3D prostoru ve zlomku vteřiny. Žádný jiný systém toto neumožňuje, pouze lidské oko je schopno rozpoznat obličej na takové úrovni. Broadway však dokáže rozpoznat obličej, ikdyž člověk jenom proběhne mezi desítkami až tisíci registrovanými uživateli. Systém si pamatuje stejně jako člověk třídimenzionální model tváře. Narozdíl od lidského oka je schopen rozpoznat i milimetrové rozdíly v 3D prostoru, pak může rozpoznat i jednovaječná dvojčata, tím se stává systém jedním z nejpřesnějších a nejbezpečnějších systému pro identifikaci. Systém dokáže zkontrolovat až 60 tváří za minutu při databázi 10 000 uživatelů.

**Obrázek 35** *3D čtečka obličejů* [40]

## 9.4 Skenování oka

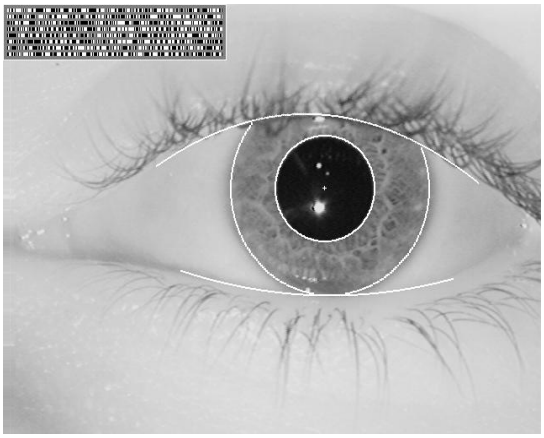
Skenování oční duhovky, nebo sítnice patří mezi nejpřesnější metody biometrie. Také z ohledu obejití tohoto systému je skenování oka jedno z nejobtížnějších, oko totiž musí být "živé", prokrvené a nejlépe ve své oční jamce. Proto se jedná z hlediska technologie o drahá zařízení.

Rozpoznávání duhovky je přesnější metodou než otisk prstů. Aby nešlo obejít systém např. fotografii oka, hlídá se i pohyb oka, roztažení zornice, nebo mrkání.

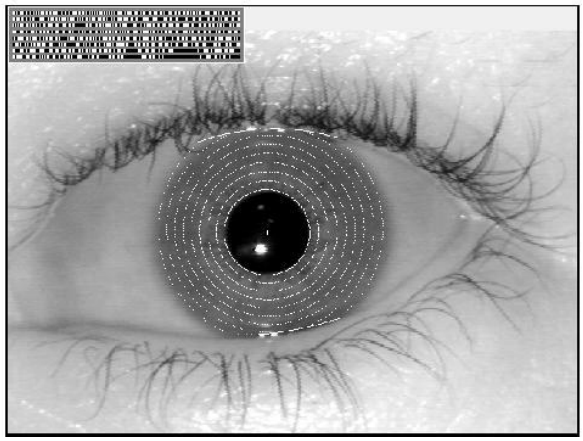
Rozpoznávání sítnice je ještě přesnější, než rozpoznávání duhovky. Struktura sítnice se snímá pomocí nízké intenzity světla v okolí slepé skvrny, což zvyšuje nároky na snímání. Uživatel se musí dívat jedním směrem do snímače. Nevýhodou je, že na sítnici může dojít ke degenerativním změnám.


**Obrázek 36** *Skenování oka* [41]

**Princip skeneru oční duhovky**: Jako první musí skener pořídit kvalitní snímek oka pomocí CCD snímače (kamery). Kamera vyfotí několik snímků s infračerveným světlem a to ve stupních šedi, tyto snímky se převedou do digitální podoby. Poté se o vše stará software, který snímky přebere, odstraní z něj přebytečné informace pomocí matematických kruhových detektorů, které najdou hranici mezi duhovkou a zornicí. Musí být vidět alespoň 50% z duhovky mezi horním a spodním víčkem, jinak je fotka detekována jako neplatná vizobrázek 37. Duhovka se rozvrhne do několika kruhových částí a převádí se do fázorových diagramů, které mají své specifické informace o poloze určitých ploch, jejich orientace a četnosti vizobrázek 38. Tyto informace jsou pomocí algoritmů převedeny do binárních kódů, které se ukládají a poté porovnávají.[42]



**Obrázek 37***Analýza fotografie duhovky* [42]



**Obrázek 38***Rozdělení duhovky do kruhů* [42]

**Skenery oční duhovky:** Nejčastější použití k identifikaci vstupu s nároky na vysokou bezpečnost. ELI-EYE2 je systém založený na platformě od LG obsahuje řídící jednotku, skener i software. Tento systém umožňuje kombinaci skenování společně s RFID ještě pro větší bezpečnost. Systém je schopný si zapamatovat až 10 000 uživatelů a snímat až ze vzdálenosti 36cm.Systém navíc umožňuje snímat i s brýlemi či kontaktními čočkami.

**Obrázek 39** *Skener oční duhovky*[43, 44]

**Biometrické skenery:**

**Výhody:**Vysoká přesnost a spolehlivost. Uživatel nemusí s sebou nosit žádná zařízení, karty ani klíče.

**Nevýhody:** Vyšší pořizovací náklady některých biometrických systému a zároveň náročnost pro okolní podmínky snímání.

**Cenová dostupnost:** cenově nejdostupnější skener otisku prstů (od 2000kč stavebnice)

**Použití pro SCX:**Nejreálnějším řešením pro použití v automobiluje skenování otisku prstů a to uvnitř vozu, jako identifikace uživatele, tedy jako náhrada za klíč a imobilizér. Skenování tváře nebo oční duhovky je náročné na okolní prostředí a počítač, který zpracovává naskenovaná data. Také z hlediska financí jsou tyto systémy dost nákladné.

# 10 Návrh zabezpečení pro elektromobil SCX

Pro návrh zabezpečení, bezkontaktního vstupu a aktivaci vozidla se musely vzít v úvahu požadavky a vlastnosti vozu, které byly stanoveny samotným elektromobilem. V tomto případě se jednalo o bezklíčové zapalování, které muselo být nahrazeno bezpečným a komfortním přístupovým systémem. Také možnost zamknout automobil při dobíjení, během kterého musí být některé elektrické obvody zapnuty, ale auto nesmí být schopno se rozjet.

## 10.1 Elektromobil StudentCar model SCX

SCX je elektromobil vyvinut a postaven týmem inženýru, profesorů, studentů a odborníků z několika firem na Vysoké škole báňské v Ostravě. Jedná se o dvoumístné kupé, které je poháněno čistě elektrickým pohonem. Poháněna jsou všechna kola, která jsou nezávisle zavěšena. O pohon se starají čtyři synchronní motory, které jsou řízeny čtyřmi frekvenčními měniči. Elektromotory jsou poháněny z 300V bateriového boxu, který je umístěn podélně středem automobilu. Použitý typ pohonu disponuje elektronickým diferenciálem a stabilizačním programem, díky tomu může automobil projíždět zatáčky vysokou rychlostí a tak dosahovat bočního přetížení přes 1G.

**Technické parametry StudentCar SCX:**

| | |
|---|---|
| Typ: | Elektromobil, dvoumístné sportovní kupé, s nezávislým pohonem všech kol |
| Výkon: | 220kW |
| Dojezd: | 180km (podle režimu jízdy) |
| Zrychlení: | 4,9s 0-100km/h<br>9,2s 0-150km/h |
| Hmotnost: | 1360kg |
| Motor: | 4x BLDC frekvenčně řízený kapalinou chlazený motor<br>Maximální točivý moment: 640N.m<br>Maximální otáčky: 1800ot./min. |
| Baterie: | 300ks LiFePO4 s kapacitou 17kWh, 320V |
| Nosný rám: | Příhradový samonosný ocelový |
| Karoserie: | Kompozitová fiberglass |
| Nápravy: | Lichoběžníkové, hnané s nezávislým pohonem kol |

## 10.2Bez klíčové zapalování

Při navrhování bez klíčové aktivace vozu se musel nahradit dosavadní aktivační systém, který byl zajištěn heslem. Heslo sice plnilo určitou míru bezpečnosti, ale z hlediska uživatele se jednalo o zdlouhavý a nekomfortní aktivační proces. Jako náhradu jsem zvolil RFID bezkontaktní čtečku s čipem, která slouží zároveň jako imobilizér.

**RFID:** (Radio Frequency Identification)- jde o bezdrátový rádio frekvenční přenos dat, při kterém nedochází ke spojení kontaktů snímače (čtečky) a identifikátoru (tagu). Tagy proto můžou být hermeticky uzavřeny v pouzdře, tudíž odolávají oxidaci, vlhkosti i prachu. Jsou tedy ideální pro provoz, navíc nepotřebují žádný zdroj energie, tu získávají ze snímače.RFID tag se skládá z čipu, kondenzátoru a antény, jeho úkolem je zachytávat impulzy vysílané komunikačním rozhraním a odpovídat na ně. Čtečkaje zařízení, které dokáže zachytit vysílaný signál aktivního, nebo pasivního čipu (tagu). Pro přenos informací má čtečka anténu. Úkolem čtečky je zpracovávat obrovské množství dat získané i od více tagů ve velmi krátkém časovém úseku.

**Instalace RFID:**Výhodou použití RFID čtečky je možnost schování celého zařízení pod palubní desku, aniž by nějaká část musela jít vidět. Aktivace probíhá přiložením čipu k určitému místu palubní desky, kde je ukryta anténa, viz obrázek 41. Pro umístění čtečky se musela vzít v úvahu i délka rozhraní, neboli kabel, po kterém je zajištěn přenos informací. V případě použití rozhraní RS232 je udávána maximální délka kabelu pro zachování rychlosti přenosu dat 15m, při větší délce už klesá přenosová rychlost dat. S použitím rozhraní USB 2.0 pro přenos dat se udává maximální délka kabelu 5m. Čip díky svým malým rozměrům se může zakomponovat do dálkového ovladače centrálního zamykání, aby k celému ovládání vozu byl jeden ovladač,vizobrázek 40. Navíc RFID čip nepotřebuje žádnou elektrickou energii, což snižuje spotřebu elektrické energie z baterie v dálkovém ovladači.


**Obrázek 40** *Ideální umístění RFID tagu (čipu)*

**Obrázek 41** *Umístění RFID čtečky v interiéru*

**Bezpečnost RFID**: Aktivační systém s použitím RFID čtečky nebude plně zabezpečen a to z důvodu možnosti naskenování RFID čipu, respektive jeho dat, díky kterým by šel automobil aktivovat. Samozřejmě se nejedná o úplně jednoduchý proces, ke kopírování čipumusí být čtecí zařízení poměrně blízko. Navíc potencionální zloděj by musel vědět, že systém funguje zrovna na RFID principu a navícpro následnou aktivaci vozu by musel vědět, kde je umístěné čtecí zařízení. Zvýšení bezpečnosti se dá dosáhnout výměnou RFID za NFC technologii, která je novější a bezpečnější. NFC pracuje na stejném principu jako RFID, tedy bezdrátový rádio frekvenční přenos dat, ovšem na bližší vzdálenost. NFC je bezpečnější než RFID, protože NFC čipy mohou být šifrovány, tedy než dojde k přenosu dat ke čtečce, probíhá nejdřív dešifrování čipu. NFC technologii využívají i bezkontaktní platební karty.

**NFC:**(Near Field Communication)- je bezdrátový přenos dat na krátkou vzdálenost, většinou pár milimetrů až centimetrů. NFC pracuje na frekvenci 13,56MHz. Vychází z principu RFID, jedná se pouze o novější technologii. Největším rozdílem je, že NFC může komunikovat oboustranně. Tedy, že data se mohou z čipu nejen číst, ale také do něj zapisovat. K zápisu dat má NFC tag paměť, jedná se tedy o paměťové zařízení s možností čtení bezdrátově. Stejně jako u RFID nepotřebuje zdroj elektrické energie, tu si tag bere pomocí elektromagnetického pole z aktivního NFC zařízení. Proto se také používá od roku 2011 v bezkontaktních platebních kartách.

Do budoucna by bylo vhodné tento systém nahradit skenerem otisku prstů, který by splňoval větší nároky na bezpečnost, navíc by se tak dalo identifikovat konkrétního uživatele. To by se dalo využít pro nastavení vozu, posunu sedačky, nebo klimatizace pro konkrétní osobu. Navíc by s elektromobilem neodjel nikdo, kdo by nebyl naveden v systému, což by výrazně zvýšilo bezpečnost proti odcizení, na rozdíl od RFID čipů, kterými se sice taky může konkrétní uživatel identifikovat, může však čip někomu zapůjčit. Na obrázku 42 můžeme vidět použití skeneru otisku prstů v upraveném prototypu Cadillac Cien, který byl postaven k výročí Cadillacu.

**Skener otisku prstů:** po přiložení prstu čtečka naskenuje otisk ve vysokém rozlišení, poté pomocí výkonného procesoru vyhodnotí důležité body, kterým následně přiřadí jedinečné ID číslo.Toto ID číslo se poté porovnává s vnitřní databází a v případě shody ho přiřadí danému uživateli.Skenovací zařízení funguje v podstatě stejně, jako čtečka RFID, pouze místo načítaní čipů dochází ke snímání otisku prstu. Také stejně jako u RFID čteček je nutné načíst do databáze otisky prstů, u některých systémů se skenují raději dva prsty, pro případ zranění, nebo velkého znečištění prstů.


**Obrázek 42** *Skener otisku prstů v interiéru(Zdroj: použité fotografie z filmu Ostrov)*

## 10.3Dálkové centrální zamykání

Pro centrální zamykání bude stačit standardní dálkové ovládání s plovoucím kódem. Prozatím automobil nebude obsahovat žádný alarm, ani vyhledávací zařízení. Dálkový ovladač centrálního zamykání poslouží zároveň jako obal pro RFID čip, se kterým bude ovladač tvořitkomplexní přístupový a aktivační systém automobilu v jednom pouzdře. Do budoucna by bylo vhodné automobil vybavit GSM/GPS alarmem, díky kterému by měl majitel neustálý dohled nad vozem. Navíc novější typy těchto alarmu umožňují ovládat některé funkce automobilu pomocí mobilního telefonu.

**GSM/GPS alarm:**je zabezpečovací systém vybavený bezdrátovým přenosem informací pomocí sítě GSM, v kombinaci s GPS může zasílat zeměpisné souřadnice automobilu. Při násilném vstupu do vozidla, nebo jeho manipulací, může alarm pomocí sítě GSM zaslat SMS zprávu majiteli, nebo bezpečnostní agentuře s informacemi, že se někdo snaží dostat do auta a to včetně zeměpisných souřadnic, kde se právě automobil nachází. Výhodou je okamžitá informovanost, ikdyž nejste v dosahu vozidla. Alarmy GSM, které jsou vybavené GPS signálem,mohou za jízdy zapisovat informace o poloze vozidla, to lze využit pro sledování firemního vozu a tvorbu knihy jízd.

Novinkou mezi GSM/GPS alarmy je komunikace s automobilem pomocí chytrého telefonu, díky kterému můžeme auto odemknout, zamknout, vyhledat, nastartovat či dokonce telefonovat s osobou ve voze.

## 10.4Návrh algoritmu

Pro správné fungování automobilu se musel navrhnout algoritmus, který bude řídit všechny elektrické obvody a tak zabrání zbytečnému vybíjení bateriového boxu, nebo pohybu vozu v době kdy se dobíjí. Také postupné zapínání a vypínání všech systémů, aby nedocházelo k přetížení stykačů, které spínají bateriový box.

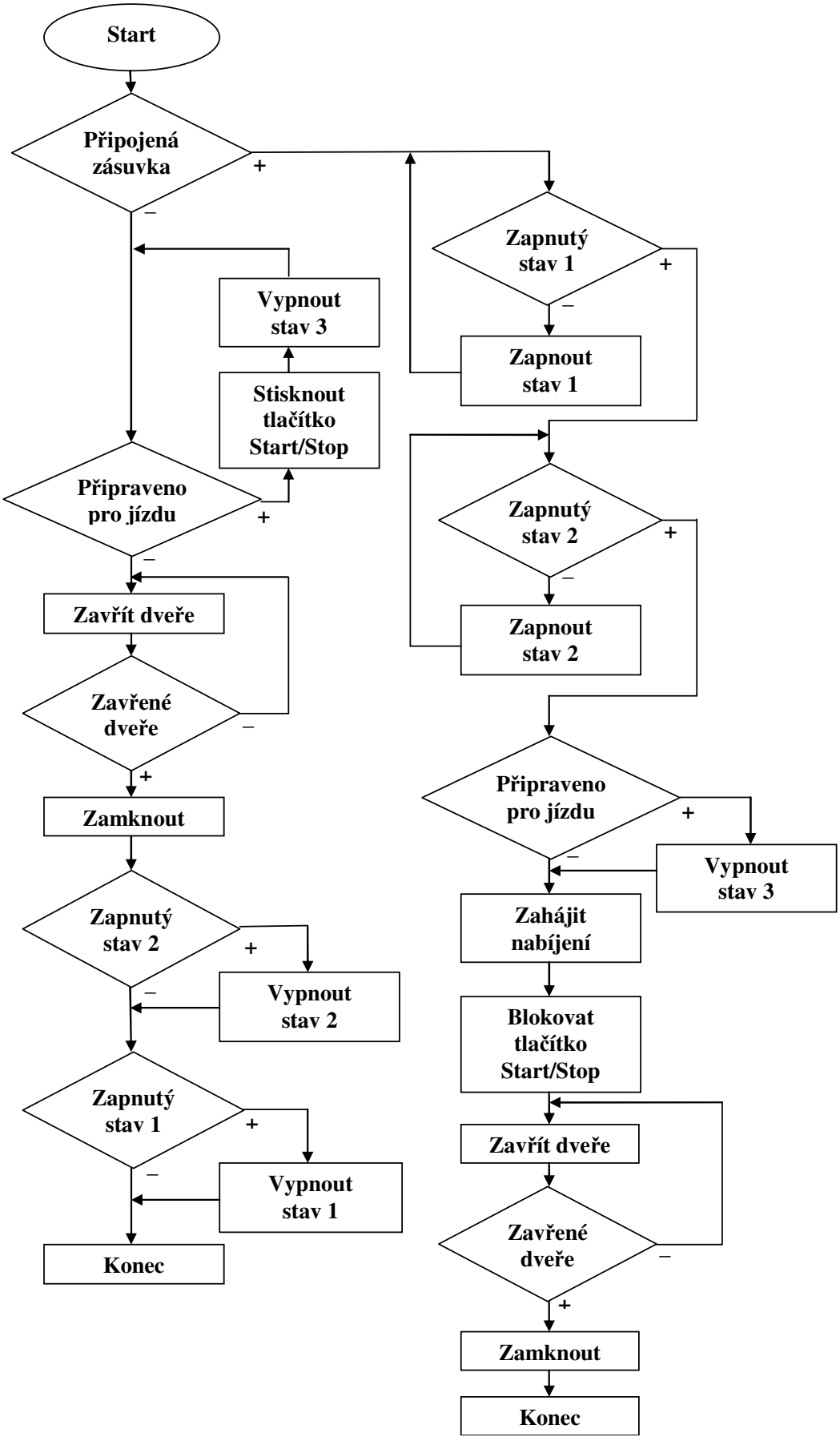
Elektromobil disponuje třemi stavy zapnutí. Stejně jako u automobilu, by se dalo říct, jsou i zde dvě polohy klíče a samotný start. Ve stavu 3 je elektromobil schopen jízdy.

Stav 1: zapnuté palubní napětí 12V (zapnutí po odemčení vozu, nebo tlačítkem Start/Stop, po 10min klidového stavu se vypne)

Stav 2: zapnutý bateriový box 300V (zapnutí tlačítkem Start/Stop, přechází ze stavu 1)

Stav 3: zapnuty měniče, čerpadla, ventilátor (zapíná automaticky ze stavu 2)

**Algoritmus pro odchod od vozu**

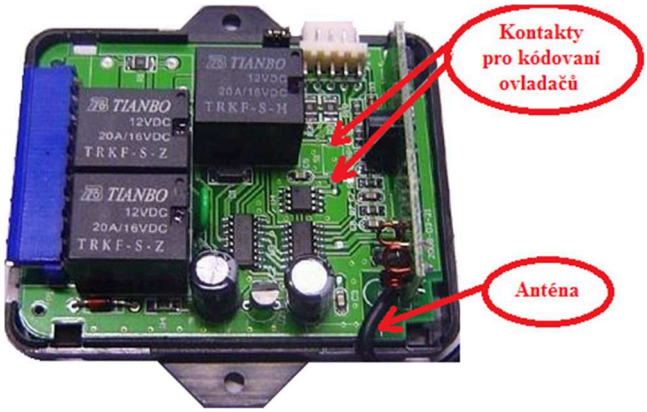


# 11 Realizace návrhu zabezpečení pro elektromobil SCX

Pro realizaci zabezpečení elektromobilu SCX jsem využil z návrhu dálkové ovládání s plovoucím kódem. Pro aktivaci vozu byla použita RFID čtečka, používaná ve škole pro identifikaci, platbu a přístup ISIC kartami.

## 11.1 Instalace dálkového ovládání

Pro realizaci bylo použité nové universální dálkové ovládání s plovoucím kódem. Jednotka se napojila na stávající centrální zamykání, odemčení a zamčení vozu je řízeno jedním vodičem připojeným na kostru buď na přímo, nebo přes rezistor 180 ohmů. Toto napojení simuluje zamykání automobilu pomocí klíče. Jednotka má výstup na automatické dovírání oken, funkci na automatické zamčení vozu, těchto funkcí se u vozu SCX prozatím nevyužilo. Funkce, kterých bylo využito, je samostatné odemykání zavazadlového prostoru, signalizace odemknutí/zamknutí vozu směrovými světly a nastavení odezvy odemknutí/zamknutí vozu, která je nastavena na 0,5s.Kódování dálkového ovladače se provádí spojením dvou kontaktů vyznačených na obrázku, poté se rozsvítí směrová světla a zmáčknutím jakéhokoliv tlačítka na dálkovém ovladači.

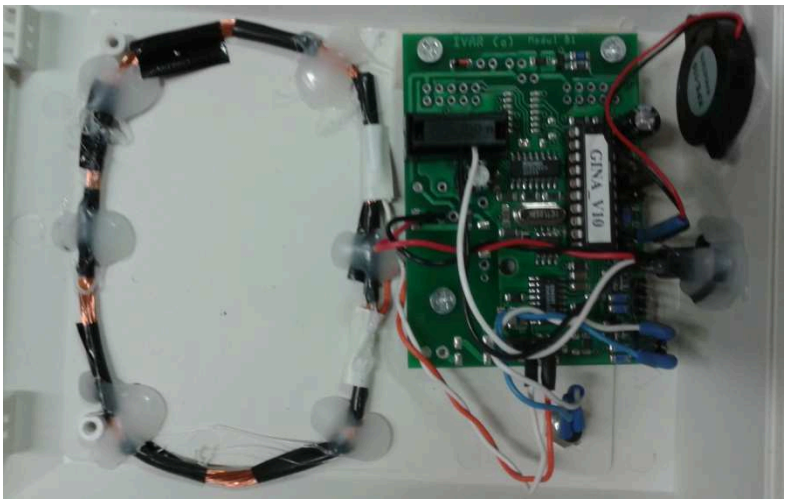



**Obrázek 43** *Jednotka dálkového ovládání centrálního zamykání*[45]


**Obrázek 44** *Dálkový ovladač*[45]

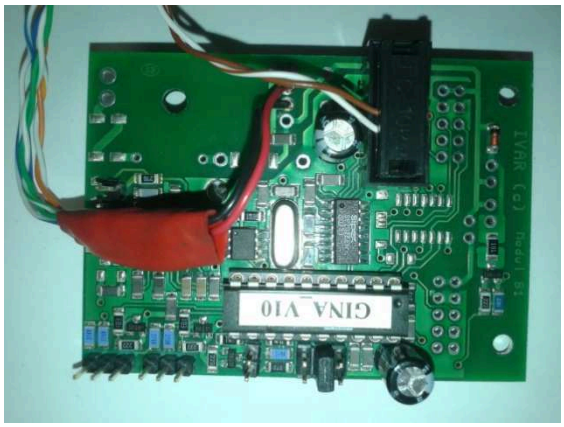
## 11.2Instalace RFID čtečky

Pro odzkoušení funkčnosti RFID technologie jako aktivační systém v automobilu se zapůjčila RFID čtečka používaná ve škole pro platbu a identifikaci ISIC kartami. Tato čtečka pracuje na frekvenci 125kHz s napájecím napětím 5V. Toto zařízení se následně upravilo pro použití do elektromobilu SCX. Plošný spoj se zabudoval do nové konstrukční krabičky a anténa se umístila do samostatného obalu pro lepší uchycení v automobilu. Výstup z RFID čtečky se upravil na konektor RS232, který se dá zapojit do řídicí jednotky. Zapůjčená RFID čtečka: v originálním obalu měla RFID čtečka signalizaci načtení tagu (čipu) led diodou a reproduktorem, obě tato indikační zařízení se pro zabudování do elektromobilu odstranila. Indikace načtení čipu bude probíhat kontrolkou pro imobilizér, nebo zvukovým tonem z tabletu.

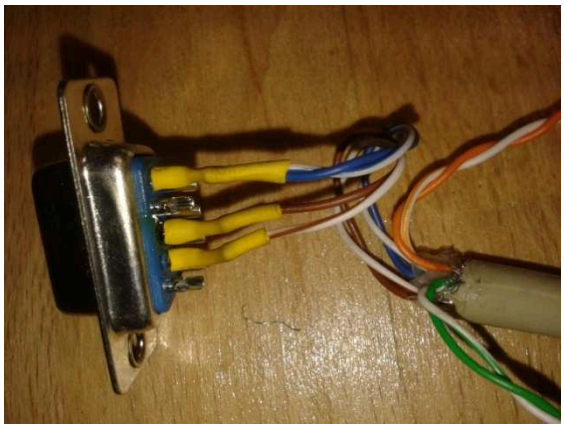



**Obrázek 45** *RFID čtečka v originální krabičce*

Výměna kabeláže a konektoru: pro použití do elektromobilu SCX se musela upravit veškerá kabeláž z důvodu původní délky vodičů a z důvodu použití jiného konektoru pro přenos dat. Pro přenos dat a napájení se použil stíněný datový kabel 4x2. Pro anténu se použila samostatná dvojlinka 2x1. Použitím konektoru RS232 je výhodou pro komunikaci mezi čtečkou a řídící jednotkou elektromobilu, to v případě RFID čteček, které fungují na principu spínání relé, není možné. Tuto komunikaci lze využít pro identifikaci konkrétního uživatele v případě, že každý řidič bude mnít svůj vlastní čip (tag), to lze využít pro nastavení vozu pro konkrétní osobu, nebo pro pozdější kontrolu kdo a kdy elektromobil řídil.

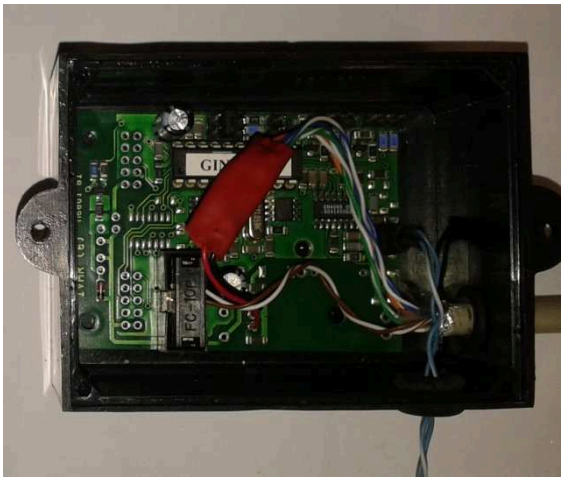



**Obrázek 46** *Plošný spoj RFID čtečky*

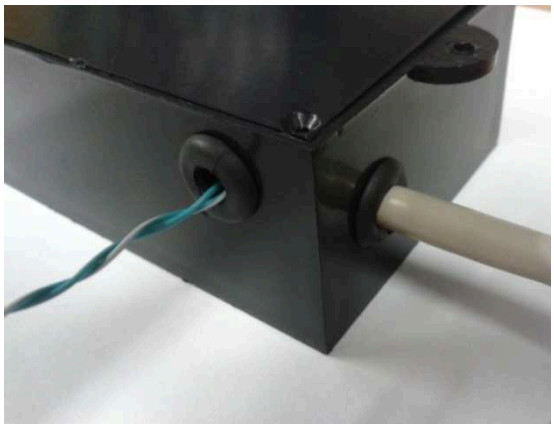


**Obrázek 47** *Konektor RS232*

Nová krabička pro RFID čtečku: z důvodu velkých rozměrů původní krabičky se musela čtečka vložit do nové krabičky, pokud možno přesně o rozměrech plošného spoje, aby zabírala co nejméně místa pod palubní deskou.

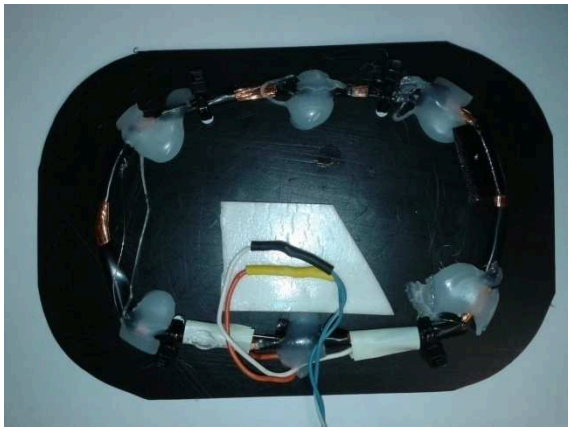


**Obrázek 48** *Nová krabička*



**Obrázek 49** *Datový a anténní kabel*

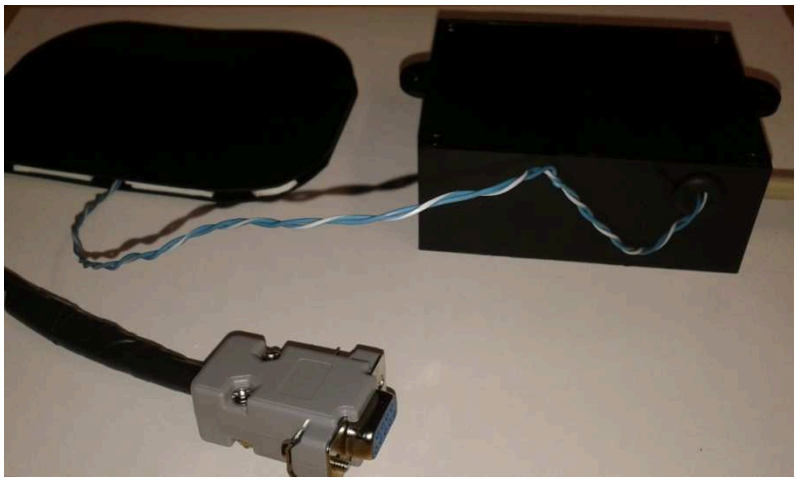
Obal pro anténu: anténa se zapouzdřila do plastového obalu proti poškození a pro lepší uchycení pod palubní desku. V tomto obalu se vyzkoušela propustnost signálu a reakce na rušící vlivy, to se zkoušelo motory v záběru, kdy v automobilu je nejvíce rušivých signálů. Mimo propustnost a rušení se také zkoušela funkčnost s použitím delšího kabelového vedení k anténě, kde se zjistilo, že námi potřebná délka kabelu nijak neovlivňuje funkčnost systému.



**Obrázek 50** *Anténa RFID čtečky*

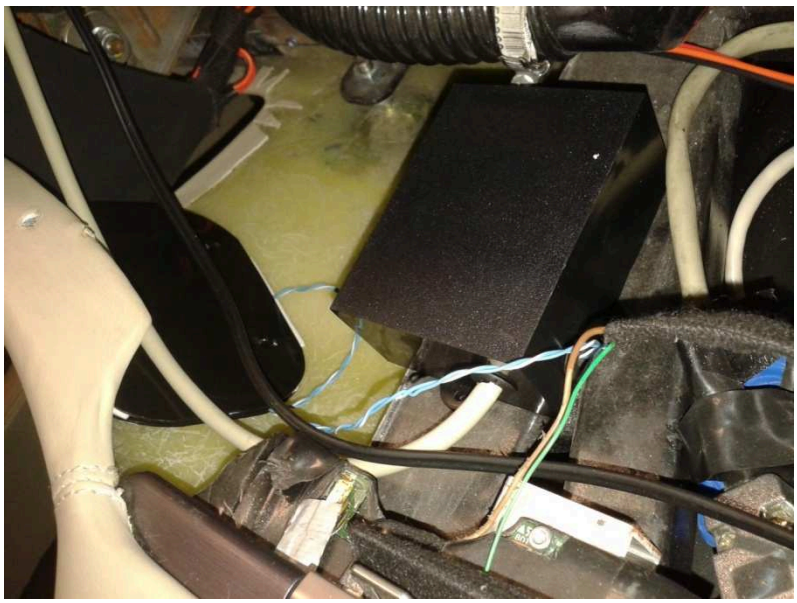
**Obrázek 51** *Obal antény RFID čtečky*

Kompletní RFID čtečka: na obrázku 52 je celé RFID zařízení, které se montovalo do elektromobilu SCX.

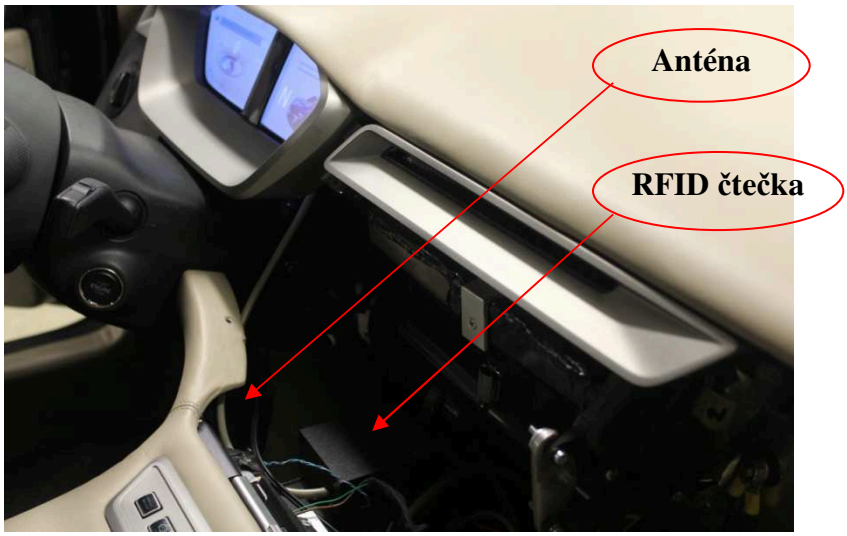


**Obrázek 52** *Kompletní RFID čtečka*

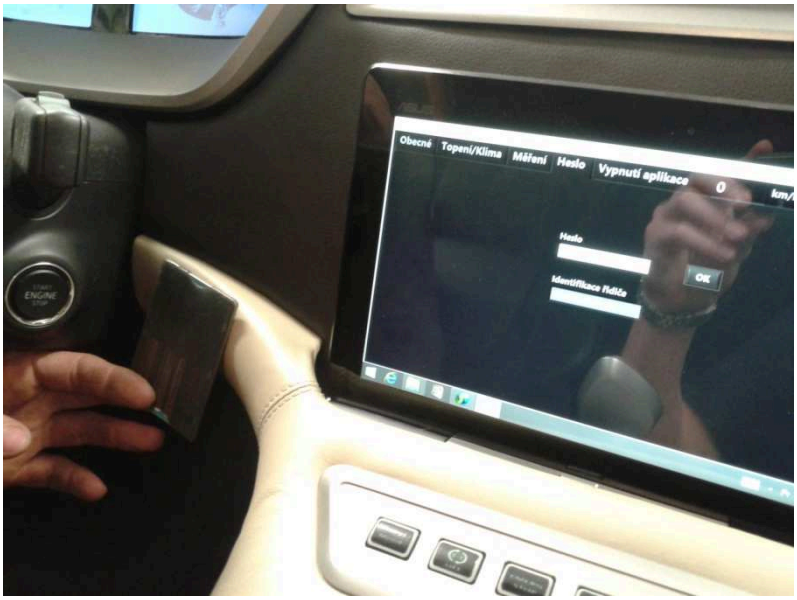
Instalace RFID čtečky do elektromobilu SCX: umístění RFID čtečky, respektive antény je podle návrhu. Anténa je přichycena ze zadní části palubní desky v místě, kde signál nestíní žádná kovová část vozidla. Čtečka je přichycena k rámu vozidla pod palubní deskou v dosahu řídící jednotky elektromobilu. RFID čtečka je odzkoušena a funkční viz obrázek 55. Aktivovat vůz, je možné buď pomocí hesla zadaného v tabletu, nebo přiložením RFID čipu (tagu) ke čtečce. Pro bezpečnost čtení RFID čipu je nutné, nezobrazovat na tabletu informace o načtení čipu v podobě kódů, nebo jiných znaků. V případě, že by tyto kódy, nebo jiné údaje spatřil někdo při aktivaci vozu, mohl by je později použít pro neoprávněnou aktivaci vozu, nebo jeho odcizení.



**Obrázek 53** *Přichycení k rámu a palubní desce*




**Obrázek 54** *Umístění čtečky v palubní desce*




**Obrázek 55** *Aktivace vozu pomocí RFID čipu (ISIC karty)*

# 12 Závěr

V prvních kapitolách jsem se věnoval běžně používaným systémům pro přístup, zabezpečení a startování vozu. Pro lepší přehled a výběr možných systému, které by se mohly instalovat do elektromobilu jsem ke každé kapitole napsal základní výhody, nevýhody, cenovou dostupnost a možnost použití pro elektromobil SCX. U každého typu zabezpečení jsem popsal možnosti překonání systému, a pokud je možnost, tak jak se proti takovému překonání bránit.

Dále jsem se zabýval technologiemi RFID a NFC, tedy bezkontaktními identifikačními systémy, které fungují na rádiových frekvencích. Tyto systémy jsem totiž chtěl použít pro bezkontaktní startování vozu, respektive jeho aktivaci. Výhodou těchto systémů je funkčnost na krátkou vzdálenost, většinou na několik centimetrů. Právě díky funkčnosti na takto krátkou vzdálenost odpadá riziko aktivace při pouhém přiblížení k vozu, jak je tomu u některých systému keyless. Další výhodou je v případě použití NFC technologie použití tagů (čipů), které mají možnost šifrování. Tyto tagy pak nelzezkopírovat čtečkou, jako u RFID, což by výrazně zvýšilo bezpečnost aktivace vozu.

Další systémy, které mě zaujaly pro použití aktivace vozu, jsou biometrické skenery, které identifikují uživatele, podle jedinečných fyziologických znaků lidského těla. Mezi ně patří např. otisk prstů, skenování tváře, ruky, oční sítnice, nebo duhovky. Těmito biometrickými systémy jsem se zabýval, protože jsem uvažoval o použití některého z těchto systému pro zabezpečení elektromobilu. Jednalo by se o prozatím jedno z nejmodernějších a zároveň nejbezpečnějších řešení aktivace vozu. Většina z těchto systémů má ovšem velké nároky na okolní prostředí, zpracování dat a také jsou dost drahé. Výjimku tvoří skener pro otisk prstů, který nemá vysoké nároky na okolní podmínky ani na zpracování dat. V podobě stavebnice ho lze zakoupit za necelé dva tisíce korun včetně skeneru i řídicí jednotky s pamětí. Výhodou takového zařízení by byla vysoká bezpečnost proti překonání. Napodobit nějakým způsobem otisk prstů, ať už získaným otiskem z předmětu, nebo již upraveným snímkem z kvalitní fotografie je velmi náročné a pro většinu lidí nereálné. Další výhodou je, že otisk prstů „nosíme“ stále u sebe, takže se nám nemůže stát, že neaktivujeme vozidlo, protože jsme někde zapomněli aktivační čip, nebo v horším případě, že nám ho někdo odcizil. I když novinkou mezi bezkontaktními technologiemi jako RFID, nebo NFC je aplikování čipu pod kůži, tedy i v tomto případě nehrozí ztráta, nebo odcizení čipu. Otázkou je, kolik lidí by bylo ochotno si nechat implantovat čip pod kůži, aby s ním mohli aktivovat svůj vůz.

V návrhu pro elektromobil jsem se věnoval možnostem použití různých systémů pro lepší zabezpečení, nebo větší pohodlí. V případě přístupu do vozu je jednou z nejlepších variant zabezpečení celkový dohled nad automobilem, pomocí alarmu s GSM/GPS. Pro aktivaci vozu jsem navrhl již zmíněné systémy RFID, nebo bezpečnější NFC. Největší bezpečnosti a komfortu by se dosáhlo se skenerem otisku prstů, který by se zabudoval do palubní desky.

Při realizaci zabezpečení a aktivace vozu jsem použil systémy z návrhu. Pro odemčení a zamčení vozu bylo použito běžné dálkové ovládání centrálního zamykání s plovoucím kódem. Dálkové ovládání se napojilo na stávající centrální zamykání a i když se jedná od dvě zařízení od jiných výrobců funguje bez sebemenších problémů. Pro aktivaci vozu byla použita RFID čtečka, běžně používaná v prostorách školy pro identifikaci ISIC kartami. Tato čtečka se následně upravila pro použití do elektromobilu. Čtečka s anténou se zapouzdřily do nových menších obalů pro lepší uchycení pod palubní desku apro komunikaci s elektromobilem se musel upravit konektor pro data na RS232. Výhodou použití RFID čtečky, která komunikuje po RS232 je možnost rozpoznání majitele, respektive konkrétního řidiče. Každý z řidičů, který vůz řídí, může mít svůj čip (tag), kterým aktivuje vůz a zároveň se identifikuje. To lze využít pro nastavení vozu pro konkrétního uživatele, nebo pro pozdější kontrolu, kdo a kdy elektromobil řídil. RFID anténa byla odzkoušena proti stínění různých materiálů, aby nedocházelo k problémům při načítání čipu pod palubní deskou.  Dále byla odzkoušená čtečka, zdali nebude docházet k rušení v případě aktivovaného auta, nebo při záběru motorů. Jediné co čtecí zařízení ovlivňovalo, bylo čtení přes kovový předmět, přes který nedošlo k načtení čipu. Proto se anténa umístila pod palubní deskou v místě, kde nebude stínit signál žádná kovová část karoserie. Instalace čtečky proběhla bez viditelných zásahů na vozidle. Testování proběhlo i po zabudování do vozidla a to během provozu. Nyní je čtecí zařízení připraveno pro běžný provoz.

# 13 Seznam použité literatury

## Seznam zdrojů:


[2]

Mechanické zabezpečení. *Auto TOPRA: Car security*[online]. 2009. vyd. [cit. 2015-05-02]. Dostupné z: http://www.topra.cz/mechanicke-zabezpeceni

[4]

Zeder lock: Recenze. *Zeder* [online]. 2015 [cit. 2015-05-02]. Dostupné z: http://www.zeder.cz/2014/05/zederlock-recenze/

[5]

Construct Savetronic. *Construct* [online]. 2015 [cit. 2015-05-02]. Dostupné z: http://www.construct.cz/produkty/construct-safetronic

[7]

Centrální zamykání. *Auto TOPRA: Car security* [online]. 2009 [cit. 2015-05-02]. Dostupné z: http://www.topra.cz/centralni-zamykani

[10]

Kessy. *Autolexicon* [online]. 2015 [cit. 2015-05-02]. Dostupné z: http://cs.autolexicon.net/articles/system-kessy-keyless-access/

[11]

Co je bezklíčový systém. *Autosme* [online]. 2009 [cit. 2015-05-02]. Dostupné z: http://auto.sme.sk/c/5041005/co-je-bezklucovy-system.html

[13]

Q-key. *Topspeed* [online]. 2013 [cit. 2015-05-02]. Dostupné z: http://www.topspeed.sk/zlodeji-maju-novinku-ukradnutie-auta-s-keyless-trva-30-sekund-/5623

[16]

Imobilizéry. *Auto TOPRA: Car security* [online]. 2009 [cit. 2015-05-02]. Dostupné z: http://www.topra.cz/elektronicke-zabezpeceni/imobilisery

[18]

Autoalarm Magicar. *Auto TOPRA: Car security* [online]. 2010 [cit. 2015-05-02]. Dostupné z:http://www.topra.cz/elektronicke-zabezpeceni/pagery/alarmy-magicar

[19]

GSM a GPS autoalarmy. *Jablotron* [online]. [cit. 2015-05-02]. Dostupné z:http://www.jablotron.com/cz/autotechnika/zabezpeceni/gsm-a-gps-autoalarmy.aspx

[21]
*Sherlog: Zabezpečení a vyhledávání* [online]. [cit. 2015-05-02]. Dostupné z: http://www.sherlog.cz
[22]
Jak funguje vyhledávání odcizených vozidel. *Carberos* [online]. 2011 [cit. 2015-05-02]. Dostupné z:http://www.carberos.cz/cz/jak-funguje-vyhledavani-vozidel/
[23]
Co je RFID. *RFID portál* [online]. [cit. 2015-05-02]. Dostupné z: http://www.rfidportal.cz/index.php?page=rfid_obecne
[26]
Obecně o RFID technologii. *Eprin* [online]. [cit. 2015-05-02]. Dostupné z: http://www.eprin.cz/rfid-technologie.html
[30]
HANAČÍK, Radim. *Bezpečnost RFID*. Brno, 2011. Dostupné z:http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=42766. Bakalářská práce. Vysoké učení technické v Brně.
[31]
*NFC mix* [online]. [cit. 2015-05-02]. Dostupné z: http://www.nfcmix.com
[32]
Biometrický identifikační systém. *Z-ware* [online]. 2006-2008 [cit. 2015-05-02]. Dostupné z: http://www.z-ware.cz/?56-biometricka-identifikace
[34]
Technologie: Bezpečnost. *Živě* [online]. 2014 [cit. 2015-05-02]. Dostupné z: http://www.zive.cz/bleskovky/hacker-zrekonstruoval-otisky-prstu-politika-pouze-z-fotek/sc-4-a-176624/default.aspx
[36]
Autentizační metody založené na biometrických informacích. *Access server* [online]. 2010 [cit. 2015-05-02]. Dostupné z:http://access.feld.cvut.cz/view.php?cisloclanku=2010110002[38]
Biometrické metody identifikace osob v bezpečnostní praxi: VŠB-TU Ostrava. [online]. 2008, s. 58 [cit. 2015-05-02]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf

[39]
JAVŮREK, Karel. 10 biometrických technologií, které vás identifikují: Technika. *VTM* [online]. [cit. 2015-05-02]. Dostupné z: http://vtm.e15.cz/aktuality/10-biometrickych-technologii-ktere-vas-identifikuji
[42]
Biometrie. *HPM* [online]. 2014 [cit. 2015-05-02]. Dostupné z:http://noel.feld.cvut.cz/vyu/a2b31hpm/index.php/Uživatel:Hlinomar

# Seznam obrázků:

[1]
*Auto Idnes* [online]. 2014 [cit. 2015-05-02]. Dostupné z: http://auto.idnes.cz/foto.aspx?r=ak_aktual&c=A140919_093129_ak_aktual_fdv&foto=FDV5602c6_SCXkopie.jpg
[3]
Páka na volant. *RR nářadí* [online]. [cit. 2015-05-02]. Dostupné z: http://www.rr-naradi.cz/paka-na-volant-s-alarmem-a-do
[4]
Zeder lock: Recenze. *Zeder* [online]. 2015 [cit. 2015-05-02]. Dostupné z: http://www.zeder.cz/2014/05/zederlock-recenze/
[6]
Mechanické zabezpečení aut. *Zabezpečené auto* [online]. [cit. 2015-05-02]. Dostupné z:http://www.zabezpeceneauto.cz/sluzby/mechanicke-zabezpeceni-aut/
[7]
Centrální zamykání. *Auto TOPRA: Car security* [online]. 2009 [cit. 2015-05-02]. Dostupné z: http://www.topra.cz/centralni-zamykani
[8]
Klíče. *Proma Uni* [online]. 2005 [cit. 2015-05-02]. Dostupné z: http://klice.unas.cz/index.php?p=klice
[9]
*Agmatronik* [online]. [cit. 2015-05-02]. Dostupné z: http://www.agmatronik.pl/kartystartowerenault
[12]
Ford Mondeo Facelift 2.0 EcoBoost. *Paultan* [online]. 2011 [cit. 2015-05-02]. Dostupné z: http://paultan.org/2011/03/09/ford-mondeo-2-0-ecoboost-powershift-short-drive/
[14]
Q-key. *Bundpol security systems* [online]. [cit. 2015-05-02]. Dostupné z: http://www.bundpol.com/oeffnungstechnik/qkey-english.htm
[15]
Prezentace modelu Škoda Superb. [online]. 2007 [cit. 2015-05-02]. Dostupné z: http://auto.xf.cz/?adresa=9
[16]
Imobilizéry. *Auto TOPRA: Car security* [online]. 2009 [cit. 2015-05-02]. Dostupné z: http://www.topra.cz/elektronicke-zabezpeceni/imobilisery

[17]
Autoalarm. *Molpir* [online]. [cit. 2015-05-02]. Dostupné z: http://shop.molpir.sk/?content=TVRDETAIL&nparams=kod_id;12105
[18]
Autoalarm Magicar. *Auto TOPRA: Car security* [online]. 2010 [cit. 2015-05-02]. Dostupné z:http://www.topra.cz/elektronicke-zabezpeceni/pagery/alarmy-magicar
[19]
GSM a GPS autoalarmy. *Jablotron* [online]. [cit. 2015-05-02]. Dostupné z:http://www.jablotron.com/cz/autotechnika/zabezpeceni/gsm-a-gps-autoalarmy.aspx
[20]
Alarm systems. *Red Chariot* [online]. [cit. 2015-05-02]. Dostupné z: http://redchariot.ie/alarm-systems/438-spy-f10s-two-way-car-alarm-with-remote-engine-start.html
[21]
*Sherlog: Zabezpečení a vyhledávání* [online]. [cit. 2015-05-02]. Dostupné z: http://www.sherlog.cz
[22]
Jak funguje vyhledávání odcizených vozidel. *Carberos* [online]. 2011 [cit. 2015-05-02]. Dostupné z:http://www.carberos.cz/cz/jak-funguje-vyhledavani-vozidel/
[24]
Zabezpečovací systémy. *CuruCZ* [online]. [cit. 2015-05-02]. Dostupné z: http://www.zabezpecovaci-system.eu/produkty/klavesnice/pc-01--pc-02-bezdotykova-rfid-karta--privesek.htm
[25]
Přístupové systémy. *Idb journal* [online]. 2012 [cit. 2015-05-02]. Dostupné z: http://www.idbjournal.sk/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878&from=rss
[27]
RFID identifikační systém. *Flajzar* [online]. [cit. 2015-05-02]. Dostupné z: http://www.flajzar.cz/elektronicke-stavebnice/rfid-identifikacni-system-pro-25-uzivatelu.htm
[28]
Aktuality. *Kodys* [online]. 2011 [cit. 2015-05-02]. Dostupné z: http://www.kodys.cz/o-nas/aktuality.html/3_732-motorola-mc9090-z-rfid-mobilni-rfid-ctecka-pro-narocne-prostredi

[29]
Zámky a příslušenství. *Goldcard* [online]. [cit. 2015-05-02]. Dostupné z: http://www.goldcard.cz/cs/hotelovy-system/zamky-a-prislusenstvi-kaba/
[32]
Biometrický identifikační systém. *Z-ware* [online]. 2006-2008 [cit. 2015-05-02]. Dostupné z: http://www.z-ware.cz/?56-biometricka-identifikace
[33]
Snímač otisku prstu. *Flajzar* [online]. [cit. 2015-05-02]. Dostupné z: http://www.flajzar.cz/pristupove-systemy/snimac-otisku-prstu-pristupovy-system.htm
[34]
Technologie: Bezpečnost. *Živě* [online]. 2014 [cit. 2015-05-02]. Dostupné z: http://www.zive.cz/bleskovky/hacker-zrekonstruoval-otisky-prstu-politika-pouze-z-fotek/sc-4-a-176624/default.aspx
[35]
Zabezpečení bytu, domu: Přístupové systémy. *České stavby* [online]. 2012 [cit. 2015-05-02]. Dostupné z:http://www.ceskestavby.cz/clanky/kam-smeruje-biometrie-21323.html
[37]
Šifrování a biometrie pod drobnohledem. *Svět hardware* [online]. 2009 [cit. 2015-05-02]. Dostupné z:http://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723-3
[38]
Biometrické metody identifikace osob v bezpečnostní praxi: VŠB-TU Ostrava. [online]. 2008, s. 58 [cit. 2015-05-02]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf
[39]
JAVŮREK, Karel. 10 biometrických technologií, které vás identifikují: Technika. *VTM* [online]. [cit. 2015-05-02]. Dostupné z: http://vtm.e15.cz/aktuality/10-biometrickych-technologii-ktere-vas-identifikuji
[40]
3D čtečky obličejů. *Biometric line* [online]. 2011-2015 [cit. 2015-05-02]. Dostupné z: http://www.biometricke-ctecky.cz/produkty/3d-ctecky-obliceju/
[41]
Biometrie. *Zprávy idnes* [online]. [cit. 2015-05-02]. Dostupné z: http://zpravy.idnes.cz/foto.aspx?r=domaci&foto1=NELfd570_oko.jpg

[42]
Biometrie. *HPM* [online]. 2014 [cit. 2015-05-02]. Dostupné z:http://noel.feld.cvut.cz/vyu/a2b31hpm/index.php/Uživatel:Hlinomar
[43]
WORRALL, John. Bezpečnost: Současný stav odvětví biometrie. *Systémy online* [online]. [cit. 2015-05-02]. Dostupné z:http://www.systemonline.cz/site/bezpecnost/rsa.htm
[44]
Biometrické skenery oka. *Biometric line* [online]. 2011-2015 [cit. 2015-05-02]. Dostupné z: http://www.biometricke-ctecky.cz/produkty/skenery-oka/
[45]
Dálkové ovládání. *Levné alarmy* [online]. 2013 [cit. 2015-05-04]. Dostupné z: http://www.levnealarmy.cz/eshop/komfortni-prvky/dalkova-ovladani/privesek-ke-klicum/dalkove-ovladani-maxicar-286-3936.html

# Seznam použitých zkratek:

| | |
|---|---|
| ŘJ | Řídicí jednotka |
| GSM | Global Systém for Mobile Communication (globální systém pro mobilní komunikaci) |
| GPS | Global Positioning Systém (globální polohový systém) |
| RFID | Radio Frequency Identification (rádio frekvenční identifikace) |
| NFC | Near Field Communication (bezdrátový přenos na krátkou vzdálenost) |
| NDEF | NFC Data Exchange Format (datový formát NFC) |
| CCD | Charge-Coupled Device (zařízení s vázanými náboji) |
| PCA | Principal Components Analysis(analýza hlavních částí) |
| LDA | Linear Discriminant Analysis(lineární diskriminační analýza) |
| EBGM | Elastic bunch graph matching (elastický srovnávací diagram) |